USC
UNIVERSIDADE DE SANTIAGO DE COMPOSTELA
FACULTADE DE MATEMÁTICAS

Traballo Fin de Grao

Bases de Groebner: Una Introducción a la Geometría Algebraica

Marcos Fernández Criado

2018 / 2019

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

GRAO DE MATEMÁTICAS

Traballo Fin de Grao

Bases de Groebner: Una Introducción a la Geometría Algebraica

Marcos Fernández Criado

2018 / 2019

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Trabajo propuesto

Área de Coñecemento: Álgebra
Título: Bases de Groebner: Introducción a la geometría algebraica
Breve descrición do contido:
Un subconjunto algebraico de un espacio afín de dimensión n sobre un cuerpo k es el conjunto soluciones de un sistema de ecuaciones polinómicas en n variables con coeficientes en el cuerpo. Estudiaremos las propiedades de este tipo de subconjuntos utilizando Bases de Gröbner. El trabajo es una propuesta para iniciar al alumno en el estudio de la Geometría Algebraica.
Recomendacións
Se recomienda haber cursado las asignaturas Ecuaciones Algebraicas, Estructuras Algebraicas. Puede ser conveniente para el alumno cursar paralelamente la asignatura Álgebra, Números y Geometría.
Outras observacións

Índice general

Resumen

En este trabajo se presentarán el lema de Dickson, los órdenes monomiales y el algoritmo de la división. Se definirán, usando el Teorema de la Base de Hilbert, y caracterizarán las bases de Groebner, y se dará un algoritmo para calcularlas: el algoritmo de Buchberger. Se resolverán dos problemas diferentes usando bases de Groebner: el problema de determinar si un polinomio pertenece a un ideal y el problema de hallar las ecuaciones implícitas de una variedad dada en forma paramétrica. Se darán también interpretaciones geométricas de resultados como el Teorema de Eliminación y el Teorema de Extensión, y aplicaciones de las bases de Groebner externas al álgebra conmutativa, tales como la resolución del problema de optimización con restricciones de una función con dominio entero, una aproximación a un algoritmo para colorear grafos con q colores y los criptosistemas Polly-Cracker para el encriptado de mensajes.

Abstract

In this paper we present Dickson‘s lemma, monomial orders and division algorithm. We define, using de Hilbert's basis theorem, and characterize Groebner bases, and provide a method to calculate them: the Buchberger‘s algorithm. We will present and solve two differente problems using Groebner bases: the ideal membership problem and the implicitization problem. Also, we will provide different geometrical interpretations of results like Elimination and Extension Theorems, and applications of Groebner bases outside commutative algebra, such as the resolution of the problem of optimize a funcion in an entire domain with constraints, an approximation of an algorithm to fill graphs with q colours and Polly-Cracker cryptosystems to code a message.

Introducción

Uno de los principales objetos de estudio de la Geometría Algebraica son las variedades algebraicas, que esencialmente se definen como el conjunto de puntos en los cuales un conjunto arbitrario de polinomios se anula.

Más concretamente, sea K un cuerpo. Denotaremos por K^n el espacio afín de dimensión n sobre el cuerpo K, y por $K[x_1, \ldots, x_n]$ el anillo de polinomios en las variables $x_1, \ldots, x_n$ con coeficientes en K. Si $S \subseteq K[x_1, \ldots, x_n]$ es un subconjunto arbitrario de polinomios, se define la variedad algebraica afín determinada por S como el conjunto

$$V(S) := \{a \in K^n : f(a) = 0 \text{ para todo } f \in S\}.$$

A la vista de esta definición, es claro que determinar los puntos que pertenecen a una variedad afín es equivalente a resolver un sistema de ecuaciones en el anillo de polinomios, es decir, las variedades establecen una relación muy directa entre los conjuntos K^n y $K[x_1, \ldots, x_n]$. Al tratar la resolución de sistemas de ecuaciones polinómicas es donde entrarán en juego las bases de Groebner.

En 1964, Groebner propuso a su estudiante Bruno Buchberger resolver el problema del cálculo de una K-base de un ideal I en $K[x_1, \ldots, x_n]$. Para su sorpresa, consiguieron desarrollar un algoritmo que era válido para cualquier ideal I. Incomprensiblemente, los resultados obtenidos por Buchberger recibieron escasa atención hasta principios de los años setenta, fue entonces cuando Buchberger acuñó el término base de Groebner. A la vez que se desarrollaba la teoría de las bases de Groebner, Hironaka (1964) introduce, aunque de modo no constructivo, las presentaciones estándar ("standard bases") para ideales en el anillo de series de potencias; estas bases han resultado ser análogas de las bases de Groebner. El trabajo de Hironaka fue independiente del de Buchberger, y no fue hasta los años setenta cuando la analogía fue sacada a la luz.

Dado un ideal del anillo de polinomios, una base de Groebner de dicho ideal consiste en un conjunto de polinomios que generan el ideal, y que además poseen otras propiedades que las hacen extremadamente interesantes, como que permiten extender el algoritmo de la división de Euclides al caso multivariante manteniendo la unicidad del resto.

Con la ayuda de estas bases, podremos llevar a cabo la resolución de cualquier sistema de ecuaciones polinómicas de una forma segura y metódica.

Para ello, en el primer capítulo introduciremos primero los ideales monomiales, que son los ideales más sencillos que podemos encontrar en el anillo de polinomios. Posteriormente, hablaremos de los órdenes monomiales, que nos permitirán definir con rigor el término principal de un polinomio. Una vez hecho esto, obtendremos el algoritmo de la división y estudiaremos los problemas que presenta en el caso multivariante. Con todos estos conceptos, estaremos en condiciones de probar el Teorema de la Base de Hilbert y de definir las bases de Groebner. Una vez definidas, estudiaremos un criterio para comprobar si un conjunto de generadores es en efecto una base de Groebner, y en caso de que no lo sea, emplearemos el algoritmo de Buchberger para, a partir de un conjunto de generadores de un ideal, conseguir otro conjunto de generadores que sea una base de Groebner.

En el segundo capítulo, relacionaremos las bases de Groebner directamente con la geometría algebraica, dando demostración al Teorema de Eliminación, al Teorema de Extensión y al Teorema de Clausura, y desarrollando un método para calcular las ecuaciones implícitas de una variedad a partir de una parametrización.

Finalmente, en el tercer capítulo introduciremos diferentes aplicaciones de las bases de Groebner a problemas matemáticos más allá de la geometría algebraica, como son el problema de optimización con restricciones de la programación lineal entera, la coloración de grafos bajo ciertas condiciones o la criptografía.

Capítulo 1

Bases de Groebner

1.1. Motivaciones: Variedades algebraicas afines.

En esta sección nos centraremos en recordar una serie de resultados vistos durante el grado que supondremos conocidos sin necesidad de demostración. Podremos consultar dichos resultados en [1] o en [2].

Observemos en primer lugar que la definición de variedad algebraica que hemos visto en la Introducción establece claramente una relación entre los conjuntos K^n y $K[x_1, \ldots, x_n]$. En lo sucesivo, escribiremos $\boldsymbol{x}$ para referirnos al conjunto de variables $x_1, \ldots, x_n$.

A partir de dicha definición, aparecen de forma natural dos aplicaciones entre los conjuntos de partes de $K[\boldsymbol{x}]$ y de K^n que serán de gran utilidad cuando estudiemos la resolución de sistemas de ecuaciones polinómicas:

$$\mathcal{P}(K[\boldsymbol{x}]) \underset{\mathbf{I}}{\overset{\mathbf{V}}{\rightleftarrows}} \mathcal{P}(K^n) \ .$$

La aplicación $\mathbf{V}$ asocia a cada subconjunto de polinomios los puntos del espacio afín en los que todos los polinomios de dicho subconjunto se anulan, mientras que la aplicación $\mathbf{I}$ asocia a cada subconjunto de puntos del espacio afín el ideal de todos los polinomios que se anulan en dichos puntos. Más rigurosamente, sean $S \in \mathcal{P}(K[\boldsymbol{x}])$ un subconjunto de polinomios en las variables $\boldsymbol{x}$, y $X \in \mathcal{P}(K^n)$ un conjunto de puntos del espacio afín. Entonces se definen las aplicaciones $\mathbf{V}$ y $\mathbf{I}$ como:

$$\mathbf{V}(S) := \{a \in K^n / f(a) = 0 \text{ para todo } f \in S\},$$

$$\mathbf{I}(X) := \{f \in K[\boldsymbol{x}] / f(a) = 0 \text{ para todo } a \in X\}.$$

Para una mayor fluidez en demostraciones de diferentes resultados que veremos más adelante, conviene mostrar primero una serie de propiedades; tanto de la aplicación $\mathbf{V}$ como de la aplicación $\mathbf{I}$:

Proposición 1.1. *Para las aplicaciones* $\boldsymbol{V}$ *e* $\boldsymbol{I}$ *que hemos definido, se cumple que*

- $\boldsymbol{V}$ *invierte el orden de inclusión: Si* $S_1 \subset S_2$*, entonces* $\boldsymbol{V}(S_2) \subset \boldsymbol{V}(S_1)$*.*
- $\boldsymbol{I}$ *invierte el orden de inclusión: Si* $X_1 \subset X_2$*, entonces* $\boldsymbol{I}(X_2) \subset \boldsymbol{I}(X_1)$*.*
- $\boldsymbol{V}(\varnothing) = K^n$*,* $\boldsymbol{V}(1) = \varnothing$*.*
- $\boldsymbol{I}(\varnothing) = K[\boldsymbol{x}]$*,* $\boldsymbol{I}(K^n) = 0$ *si, y sólo si,* K *es infinito.*
- *Si* V *es una variedad afín,* $\boldsymbol{V}(\boldsymbol{I}(V)) = V$*.*

Corolario 1.2. *La composición de las aplicaciones* $\boldsymbol{I}$ *y* $\boldsymbol{V}$ *no invierte el orden de inclusión: Si* $X_1 \subset X_2$ *entonces* $\boldsymbol{V}(\boldsymbol{I}(X_1)) \subset \boldsymbol{V}(\boldsymbol{I}(X_2))$*, y si* $S_1 \subset S_2$ *entonces* $\boldsymbol{I}(\boldsymbol{V}(S_1)) \subset \boldsymbol{I}(\boldsymbol{V}(S_2))$

A continuación, definimos una topología en la que las variedades afines ocupan una posición destacada, y de esta forma podremos utilizar las propiedades de dicha topología para estudiar su comportamiento.

Definición 1.3. La topología de Zariski de K^n, es la topología cuyos cerrados son los conjuntos de puntos que son ceros comunes a un conjunto de polinomios.

Definición 1.4. Sea $X \subset K^n$ un subconjunto del espacio afín de dimensión n. La clausura de X respecto a la topología de Zariski es la menor variedad afín que contiene al conjunto X.

Esto nos indica la estrecha relación que hay entre la topología de Zariski y las aplicaciones $\mathbf{I}$ y $\mathbf{V}$:

Proposición 1.5. *Sea* $X \subset K^n$*. La variedad afín* $\boldsymbol{V}(\boldsymbol{I}(X))$ *es la clausura de Zariski de* X*, es decir, es la menor variedad que contiene a* X*.*

Demostración. Sea W una variedad afín arbitraria que contiene a X. Tenemos que probar que $\mathbf{V}(\mathbf{I}(X)) \subset W$.

Como $X \subset W$, dado que tanto la aplicación $\mathbf{I}$ como la aplicación $\mathbf{V}$ invierten el orden de las inclusiones, se tiene que $\mathbf{I}(W) \subset \mathbf{I}(X)$ y que $\mathbf{V}(\mathbf{I}(W)) \subset \mathbf{V}(\mathbf{I}(S))$. Ahora bien, como W es una variedad, $\mathbf{V}(\mathbf{I}(W)) = W$ y entonces $W \subset \mathbf{V}(\mathbf{I}(S))$ como queríamos demostrar. □

A lo largo de los diferentes capítulos, consideraremos polinomios en el anillo $K[x_1, \ldots, x_n]$. Al considerar más de una variable, surgen de forma natural diferentes problemas con los que no era necesario lidiar en el caso de una sola variable.

Sin ir más lejos, el anillo de polinomios en la variable x sobre el cuerpo K, $K[x]$ es un dominio de ideales principales, mientras que $K[x_1, \ldots, x_n]$ es un dominio de factorización

única, pero no de ideales principales: si consideramos el ideal $I = \langle x_1, x_2 \rangle$, resulta evidente darse cuenta de que no podemos generar el ideal con un único polinomio.

Otra de las dificultades que nos encontramos al trabajar con ideales de polinomios en varias variables es lo que llamaremos *Problema de la descripción de ideales*, que consiste en lo siguiente: Dado un ideal $I \subset K[x_1, \ldots, x_n]$, ¿existe siempre un conjunto finito de generadores de I? Es decir, ¿existen $f_1, \ldots, f_s$ tales que $I = \langle f_1, \ldots, f_s \rangle$? Además, en el caso de que tengamos un conjunto de generadores de un ideal, $I = \langle f_1, \ldots, f_s \rangle$, ¿Podemos determinar si un polinomio dado f pertenece al ideal?

Por último, necesitamos hablar de un tipo particular de ideales, denominados ideales radicales, que también tienen relación con las aplicaciones **I** y **V**:

Definición 1.6. Sea $I \subset K[x_1, \ldots, x_n]$ un ideal. El conjunto

$$\sqrt{I} := \{f \in K[x_1, \ldots, x_n] \ / \ \exists n \in \mathbb{N}, f^n \in I\}$$

se denomina radical del ideal I.

Proposición 1.7. *Dado un ideal I, $\sqrt{I}$ es también un ideal.*

Definición 1.8. Un ideal I se dice radical si coincide con su radical, es decir, si $I = \sqrt{I}$.

Lema 1.9 (Teorema de los ceros de Hilbert)**.** *Sea K un cuerpo algebraicamente cerrado. Si el polinomio $f \in K[\boldsymbol{x}]$ verifica que $f \in \boldsymbol{I}(\boldsymbol{V}(f_1, \ldots, f_s))$, entonces existe un entero $m \geqslant 1$ tal que $f^m \in \langle f_1, \ldots, f_s \rangle$.*

La demostración de este último resultado puede consultarse en [4]. Este teorema también puede enunciarse como sigue: Si K es un cuerpo algebraicamente cerrado, e $I = \langle f_1, \ldots, f_s \rangle$, entonces

$$\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}.$$

1.2. Ideales monomiales: Lema de Dickson.

En esta sección vamos a resolver el **Problema de la descripción de ideales** para un tipo concreto de ideales: Los ideales monomiales. Este caso particular es uno de los ingredientes que nos permitirá resolver el problema en general.

Los polinomios de la forma $cx_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n} \in K[x_1,\ldots,x_n]$, con $\boldsymbol{\alpha} = (\alpha_1,\alpha_2,\ldots,\alpha_n) \in \mathbb{N}^n$ y $c \in K$ un escalar no nulo, se denominan monomios; el (múlti-)grado $\boldsymbol{\alpha} = (\alpha_1,\ldots,\alpha_n)$ determina el monomio $x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}$. Para él utilizaremos la notación abreviada

$$\boldsymbol{x}^{\boldsymbol{\alpha}} = x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}.$$

El anillo de polinomios $K[\boldsymbol{x}] = K[x_1,\ldots,x_n]$ es un K-espacio vectorial y el conjunto de *los monomios mónicos* $\mathcal{M}(x_1,\ldots,x_n) = \{\boldsymbol{x}^{\boldsymbol{\alpha}} \,/\, \boldsymbol{\alpha} \in \mathbb{N}^n\}$ es la base canónica de $K[\boldsymbol{x}]$.

El conjunto $\mathcal{M}(\boldsymbol{x}) = \mathcal{M}(x_1,\ldots,x_n)$ es un monoide con el producto de $K[\boldsymbol{x}]$, y la correspondencia $\boldsymbol{x}^? \colon \mathbb{N}^n \to \mathcal{M}(\boldsymbol{x})$ es un isomorfismo entre los monoides $(\mathbb{N}^n,+)$ y $(\mathcal{M}(\boldsymbol{x}),\cdot)$. Denotaremos $\mathbf{0} = (0,\ldots,0)$ el neutro de $\mathbb{N}^n$, que corresponde al neutro $1 \in \mathcal{M}(\boldsymbol{x})$.

Definición 1.10. Diremos que un ideal $I \subset K[x_1,\ldots,x_n]$ es *monomial* si posee un sistema de generadores formado por monomios, o equivalentemente (por ser K un cuerpo), si existe un subconjunto $A \subset \mathbb{N}^n$ tal que $I = \langle \boldsymbol{x}^{\boldsymbol{\alpha}} \;/\; \alpha \in A\rangle$, esto es:

$$f \in I \quad\Longleftrightarrow\quad f = \sum_{i=1}^{s} h_i \boldsymbol{x}^{\boldsymbol{\alpha}(i)},\ \text{con } \boldsymbol{\alpha}(i) \in A \text{ y } h_i \in K[x_1,\ldots,x_n]$$

Proposición 1.11. *sea I un ideal monomial y $f \in K[x_1,\ldots,x_n]$ un polinomio. Los siguientes enunciados son equivalentes:*

- *(i) El polinomio f pertenece a I.*
- *(ii) Cada monomio de f pertenece a I.*
- *(iii) El polinomio f es una combinación K-lineal de monomios de I.*

Demostración. Las implicaciones $(iii) \Rightarrow (ii) \Rightarrow (i)$ son consecuencia inmediata de la definición de ideal monomial. Para completar la demostración veamos que $(i) \Rightarrow (iii)$. Supongamos que $I = \langle \boldsymbol{x}^{\boldsymbol{\alpha}} \;/\; \alpha \in A\rangle$ para un subconjunto $A \subset \mathbb{N}^n$. Entonces cada polinomio $f \in I$ se puede escribir de la forma $f = \sum_{i=1}^{s} h_i \boldsymbol{x}^{\boldsymbol{\alpha}(i)}$, para ciertos exponentes $\boldsymbol{\alpha}(i) \in A$ y polinomios $h_i \in K[x_1,\ldots,x_n]$. Escribiendo cada polinomio h_i como combinación K-lineal de monomios, $h_i = \sum_{j=1}^{s_i} b_{ij}\boldsymbol{x}^{\boldsymbol{\nu}(ij)}$, se obtiene una expresión de la forma

$$f = \sum_{i=1}^{s} h_i \boldsymbol{x}^{\boldsymbol{\alpha}(i)} = \sum_{i=1}^{s}\sum_{j=1}^{s_i} b_{ij}\boldsymbol{x}^{\boldsymbol{\nu}(ij)}\boldsymbol{x}^{\boldsymbol{\alpha}(i)}, \tag{1.1}$$

es decir, f se escribe como combinación K-lineal de monomios $\boldsymbol{x}^{\boldsymbol{\nu}(ij)}\boldsymbol{x}^{\boldsymbol{\alpha}(i)} \in I$. □

Corolario 1.12. *Dos ideales monomiales son iguales si, y sólo si, contienen los mismos monomios.*

Lema 1.13. *Sea* $I = \langle \boldsymbol{x}^{\boldsymbol{\alpha}} \,/\, \boldsymbol{\alpha} \in A \rangle \subset K[x_1, \ldots, x_n]$ *un ideal monomial, con* $A \subset \mathbb{N}^n$*. Dado* $\boldsymbol{\sigma} \in \mathbb{N}^n$ *equivalen:*

(*i*) *El monomio* $\boldsymbol{x}^{\boldsymbol{\sigma}}$ *pertenece a* I*.*

(*ii*) *El monomio* $\boldsymbol{x}^{\boldsymbol{\sigma}}$ *es divisible por* $\boldsymbol{x}^{\boldsymbol{\alpha}}$ *para algún* $\boldsymbol{\alpha} \in A$*.*

(*iii*) *Existe* $\boldsymbol{\alpha} \in A$ *tal que* $\boldsymbol{\sigma} = \boldsymbol{\alpha} + \boldsymbol{\nu}$*, para algún* $\boldsymbol{\nu} \in \mathbb{N}^n$*.*

Demostración. Las implicaciones (*iii*) $\Rightarrow$ (*ii*) $\Rightarrow$ (*i*) son inmediatas. Para demostrar que (*i*) $\Rightarrow$ (*iii*) supongamos que $f = \boldsymbol{x}^{\boldsymbol{\sigma}}$ en la expresión (1.1), entonces agrupando los términos de la derecha se tendría que $\boldsymbol{x}^{\boldsymbol{\sigma}}$ es una suma finita de términos de la forma $b_{ij}\boldsymbol{x}^{\boldsymbol{\nu}_{ij}+\boldsymbol{\alpha}_i}$. Por ser los monomios una K-base la suma de la derecha se reduce a un término de la forma $\boldsymbol{x}^{\boldsymbol{\nu}+\boldsymbol{\alpha}}$ con $\boldsymbol{\alpha} \in A$ y $\boldsymbol{\nu} \in \mathbb{N}^n$. □

El *Lema de Dickson* resuelve el **Problema de la descripción de ideales** para el caso de ideales monomiales: *Todo ideal monomial del anillo de polinomios* $K[x_1, \ldots, x_n]$ *es finitamente generado.* En lugar de demostrar directamente el *Lema de Dickson*, enunciaremos y demostraremos un resultado equivalente sobre los exponentes de los monomios de un ideal monomial (Proposición 1.14), obteniendo como corolario inmediato el *Lema de Dickson.*

Consideremos en $\mathbb{N}^n$ la relación determinada "componente a componente" a partir de la relación de orden habitual de $\mathbb{N}$, es decir, la relación de orden definida de la siguiente forma:

$$\boldsymbol{\alpha} \ll \boldsymbol{\sigma} \quad :\Longleftrightarrow \quad \boldsymbol{\sigma} - \boldsymbol{\alpha} \in \mathbb{N}^n \qquad (\boldsymbol{\alpha},\, \boldsymbol{\sigma} \in \mathbb{N}^n) \tag{1.2}$$

Si denotamos $\boldsymbol{\alpha} + \mathbb{N}^n := \{\boldsymbol{\alpha} + \boldsymbol{\nu} \,/\, \boldsymbol{\nu} \in \mathbb{N}^n\}$,

$$\boldsymbol{\alpha} \ll \boldsymbol{\sigma} \quad \Longleftrightarrow \quad \boldsymbol{\sigma} \in \boldsymbol{\alpha} + \mathbb{N}^n.$$

- El orden $\ll$ es compatible con la estructura de monoide $(\mathbb{N}^n, +)$:

$$\forall\, \boldsymbol{\alpha},\, \boldsymbol{\sigma},\, \boldsymbol{\nu} \in \mathbb{N}^n : \qquad \boldsymbol{\alpha} \ll \boldsymbol{\sigma} \quad \Longrightarrow \quad \boldsymbol{\alpha} + \boldsymbol{\nu} \ll \boldsymbol{\sigma} + \boldsymbol{\nu} \tag{1.3}$$

- Si $n > 1$ entonces $(\mathbb{N}^n, \ll)$ no es un conjunto bien ordenado, pero tiene la siguiente buena propiedad:

Proposición 1.14 (Lema de Dickson para $\mathbb{N}^n$)**.** *En el conjunto ordenado* $(\mathbb{N}^n, \ll)$*, todo subconjunto* $A \subset \mathbb{N}^n$ *no vacío posee un número finito de elementos minimales.*

Demostración. Haremos la demostración por inducción en n. El caso $n = 1$ es la propiedad del buen orden de los naturales. Supongamos que $n > 1$. Elegimos un elemento $\boldsymbol{\alpha}(0) = (\alpha_{01}, \alpha_{02}, \ldots, \alpha_{0n}) \in A$, si existe $\boldsymbol{\sigma} \in A$ tal que $\boldsymbol{\sigma} \notin \boldsymbol{\alpha}(0) + \mathbb{N}^n$, entonces existirá un índice $i \in \{1, \ldots, n\}$ para el cual $\sigma_i < \alpha_{0i}$. Es decir, $\boldsymbol{\sigma} \in \cup_{i=1}^{n} A_i$, donde

$$A_i := \{\boldsymbol{\alpha} \in A \ / \ 0 \leqslant \alpha_i < \alpha_{0i}\}, \quad i \in \{1, \ldots, n\}.$$

Obsérvese que $A_i = \bigcup_{0 \leqslant j < \alpha_{0i}} A_{ij}$, siendo $A_{ij} := \{\boldsymbol{\alpha} \in A_i \ / \, \alpha_i = j \, \}$. Sea $\pi_i \colon \mathbb{N}^n \to \mathbb{N}^{n-1}$ la proyección que consiste en eliminar la componente $i \in \{1, \ldots, n\}$. La proyección π_i induce una biyección que conserva el orden entre A_{ij} y su imagen $\pi_i(A_{ij}) \subset \mathbb{N}^{n-1}$. Por hipótesis de inducción, si A_{ij} es no vacío entonces posee un conjunto finito de elementos minimales A_{ij}; sea A_0 la unión de la colección finita de subconjuntos A_{ij}. Entonces $A = \{\boldsymbol{\alpha}(0)\} \cup A_0 \subset A$ es un subconjunto finito que contiene todos los minimales de A. □

Según el Lema 1.13, la relación $\boldsymbol{\alpha} \ll \boldsymbol{\sigma}$ equivale a que el monomio $\boldsymbol{x}^{\boldsymbol{\sigma}}$ sea divisible por el monomio $\boldsymbol{x}^{\boldsymbol{\alpha}}$, y se tiene la siguiente consecuencia de la proposición:

Corolario 1.15 (Lema de Dickson)**.** *Sea $A \subset \mathbb{N}^n$ e $I = \langle \boldsymbol{x}^{\boldsymbol{\alpha}} \, / \, \boldsymbol{\alpha} \in A \rangle \subset K[\boldsymbol{x}]$ el ideal monomial que determina A. Existen $\boldsymbol{\alpha}(1), \ldots, \boldsymbol{\alpha}(s) \in A$ tales que $I = \langle \boldsymbol{x}^{\boldsymbol{\alpha}(1)}, \ldots, \boldsymbol{x}^{\boldsymbol{\alpha}(s)} \rangle$.*

Demostración. Según la proposición anterior, respecto a la relación de orden $\ll$, el conjunto A posee un conjunto finito de minimales. Si $\boldsymbol{\alpha}(1), \ldots, \boldsymbol{\alpha}(s)$ son los minimales de A entonces $A \subset \cup_{i=1}^{s} (\, \boldsymbol{\alpha}(i) + \mathbb{N}^n \,)$ y, por el Lema 1.13, $I = \langle \boldsymbol{x}^{\boldsymbol{\alpha}(1)}, \ldots, \boldsymbol{x}^{\boldsymbol{\alpha}(s)} \rangle$. □

1.3. Órdenes monomiales.

En el anillo de polinomios en una variable $K[x]$, sobre un cuerpo K, la ordenación de monomios

$$\cdots > x^{m+1} > x^m > \cdots > x^2 > x > 1$$

es un elemento clave en el *algoritmo de la división*. También se ordenan las variables en el *algoritmo de reducción de Gauss* para resolver sistemas de ecuaciones lineales en varias variables $x_1, \ldots, x_n$ con coeficientes en K.

En estos algoritmos, cada iteración se reduce a trabajar con "el coeficiente principal" de los polinomios. Si queremos generalizar estos algoritmos para tratar de resolver sistemas de ecuaciones con coeficientes en el cuerpo K que involucran varias variables, $x_1, \ldots, x_n$, elevadas a exponentes naturales arbitrarios, nos encontramos con un problema evidente: ¿Cuál es el coeficiente principal de un polinomio no nulo $f \in K[x_1, \ldots, x_n]$?

En $K[x]$ el orden de los monomios $\mathcal{M}(x)$ es claro, se ordenan según los exponentes siguiendo el orden de $\mathbb{N}$. Esta forma de ordenar los monomios de $\mathcal{M}(x)$ posee dos propiedades muy útiles: es un *buen orden* y es *compatible con el producto de monomios*. El objetivo en esta sección es ordenar el conjunto de los monomios $\mathcal{M}(\boldsymbol{x}) \subset K[\boldsymbol{x}] = K[x_1, \ldots, x_n]$ de forma que se verifiquen esas *buenas propiedades*.

A través de la correspondencia biyectiva $\boldsymbol{x}^? \colon \mathbb{N}^n \to \mathcal{M}(\boldsymbol{x})$, dar un orden en el conjunto $\mathcal{M}(\boldsymbol{x})$ equivale a dar un orden en el conjunto de los exponentes $\mathbb{N}^n$. Si $\leqslant$ es una relación de orden en $\mathbb{N}^n$, denotaremos con el mismo símbolo $\leqslant$ el orden determinado en $\mathcal{M}(\boldsymbol{x})$:

$$\boldsymbol{x}^{\boldsymbol{\alpha}} \leqslant \boldsymbol{x}^{\boldsymbol{\sigma}} \quad :\Longleftrightarrow \quad \boldsymbol{\alpha} \leqslant \boldsymbol{\sigma} \qquad (\boldsymbol{\alpha}, \boldsymbol{\sigma} \in \mathbb{N}^n).$$

Como la correspondencia $\boldsymbol{x}^? \colon \mathbb{N}^n \to \mathcal{M}(\boldsymbol{x})$ es un isomorfismo de monoides entre $(\mathbb{N}^n, +)$ y $(\mathcal{M}(\boldsymbol{x}), \cdot)$, que un orden en $\mathbb{N}^n$ sea compatible con la suma equivale a que el determinado en $\mathcal{M}(\boldsymbol{x})$ sea compatible con el producto.

Ejemplo 1.16. El orden $(\mathbb{N}^n, \ll)$, definido en (1.2), determina la ordenación de monomios

$$\boldsymbol{x}^{\boldsymbol{\alpha}} \ll \boldsymbol{x}^{\boldsymbol{\sigma}} \quad :\Longleftrightarrow \quad \boldsymbol{\alpha} \ll \boldsymbol{\sigma}.$$

Como hemos indicado, este no en un *buen orden* si $n > 1$; sin embargo, el orden $(\mathbb{N}^n, \ll)$ es compatible con la suma, es decir, el orden que determina entre los monomios $\mathcal{M}(\boldsymbol{x})$ es compatible con el producto:

$$\forall\, \boldsymbol{\alpha}, \boldsymbol{\sigma}, \boldsymbol{\nu} \in \mathbb{N}^n : \qquad \boldsymbol{x}^{\boldsymbol{\alpha}} \ll \boldsymbol{x}^{\boldsymbol{\sigma}} \quad \Longleftrightarrow \quad \boldsymbol{x}^{\boldsymbol{\alpha}} \boldsymbol{x}^{\boldsymbol{\nu}} \ll \boldsymbol{x}^{\boldsymbol{\sigma}} \boldsymbol{x}^{\boldsymbol{\nu}}$$

La siguiente definición resume las propiedades que dede tener un orden en el conjunto de exponentes $\mathbb{N}^n$ para que el orden que establece entre monomios $\mathcal{M}(\boldsymbol{x})$ tenga "buenas propiedades":

Definición 1.17. Un orden $\leqslant$ en $\mathbb{N}^n$ es *monomial* si es un buen orden que, además, es compatible con la suma, es decir, $\forall\, \boldsymbol{\alpha}$, $\boldsymbol{\sigma}$ y $\boldsymbol{\nu} \in \mathbb{N}^n$ se verifica $[\ \boldsymbol{\alpha} \leqslant \boldsymbol{\sigma} \implies \boldsymbol{\alpha}+\boldsymbol{\nu} \leqslant \boldsymbol{\sigma}+\boldsymbol{\nu}\ ]$.

Lema 1.18. *Una relación de orden $\leqslant$ en $\mathbb{N}^n$ es un buen orden si, y sólo si, toda sucesión decreciente de elementos de $\mathbb{N}^n$,*

$$\boldsymbol{\alpha}(1) \geqslant \boldsymbol{\alpha}(2) \geqslant \boldsymbol{\alpha}(3) \geqslant \cdots\ ,$$

es estacionaria, es decir, existe $n \in \mathbb{N}$ tal que $\boldsymbol{\alpha}(n) = \boldsymbol{\alpha}(m)$ para todo $m \geq n$.

Demostración. Demostraremos que $\leqslant$ no es un buen orden si, y sólo si, existe una sucesión infinita estrictamente decreciente de elementos de $\mathbb{N}^n$.

Si $\leqslant$ no es un buen orden en $\mathbb{N}^n$, existirá un subconjunto no vacío $S \subset \mathbb{N}^n$ que no tiene elemento mínimo. Como S es no vacío, podemos elegir un elemento $\boldsymbol{\alpha}(1) \in S$; como $\boldsymbol{\alpha}(1)$ no es mínimo de S, existirá un elemento $\boldsymbol{\alpha}(2) \in S$ tal que $\boldsymbol{\alpha}(1) > \boldsymbol{\alpha}(2)$; como $\boldsymbol{\alpha}(2) \in S$ no es el mínimo de S, existirá un elemento $\boldsymbol{\alpha}(3) \in S$ tal que $\boldsymbol{\alpha}(2) > \boldsymbol{\alpha}(3)$. Repitiendo este proceso construímos una sucesión infinita estrictamente decreciente de elementos de $\mathbb{N}^n$.

Recíprocamente, si existe una sucesión estrictamente decreciente de elementos de $\mathbb{N}^n$

$$\boldsymbol{\alpha}(1) > \boldsymbol{\alpha}(2) > \boldsymbol{\alpha}(3) > \cdots$$

entonces el subconjunto $S = \{\boldsymbol{\alpha}(1), \boldsymbol{\alpha}(2), \boldsymbol{\alpha}(3), \ldots\} \subset \mathbb{N}^n$ es no vacío y no posee mínimo, así que $\leqslant$ no puede ser un buen orden. □

Antes de entrar en más detalles, vamos a presentar un corolario útil de la Proposición 1.14 (Lema de Dickson para $\mathbb{N}^n$) que permite caracterizar de forma más sencilla los ordenes monomiales.

Corolario 1.19. *Sea $\leqslant$ una relación de orden en $\mathbb{N}^n$ verificando:*

(i) $\leqslant$ es una realación de orden total.

(ii) $\leqslant$ es compatible con la suma de $\mathbb{N}^n$.

Entonces, $\leqslant$ es un buen orden en $\mathbb{N}^n$ si, y sólo si, $\boldsymbol{\alpha} \geqslant \mathbf{0} = (0, \ldots, 0)$ para cualquier $\boldsymbol{\alpha} \in \mathbb{N}^n$.

Demostración. Asumiendo que $(\mathbb{N}^n, \leqslant)$ es un conjunto bien ordenado es suficiente comprobar que $\boldsymbol{\beta} \geqslant \mathbf{0}$, siendo $\boldsymbol{\beta}$ el elemento más pequeño de $\mathbb{N}^n$. Supongamos que $\boldsymbol{\beta} \ngeqslant \mathbf{0}$, como la relación de orden es total necesariamente $\mathbf{0} > \boldsymbol{\beta}$; entonces por (ii) se tiene que $\boldsymbol{\beta} = \mathbf{0} + \boldsymbol{\beta} > \boldsymbol{\beta} + \boldsymbol{\beta}$, lo cual es un absurdo dado que $\boldsymbol{\beta} + \boldsymbol{\beta} \in \mathbb{N}^n$ y $\boldsymbol{\beta}$ era el elemento más pequeño de $\mathbb{N}^n$.

Recíprocamente, supongamos que $\boldsymbol{\alpha} \geqslant \mathbf{0}$, $\forall\, \boldsymbol{\alpha} \in \mathbb{N}^n$. Obsérvese que en este caso:

$$\boldsymbol{\alpha} \ll \boldsymbol{\sigma} \quad \Longrightarrow \quad \boldsymbol{\alpha} \leqslant \boldsymbol{\sigma} \qquad (\boldsymbol{\alpha}, \boldsymbol{\sigma} \in \mathbb{N}^n)$$

En efecto, por hipótesis $\mathbf{0}$ es el mínimo de $(\mathbb{N}^n, \leqslant)$ y $\leqslant$ es compatible con la suma entonces

$$\boldsymbol{\alpha} \ll \boldsymbol{\sigma} \quad \Longleftrightarrow \quad \boldsymbol{\sigma} - \boldsymbol{\alpha} \in \mathbb{N}^n \quad \Longrightarrow \quad \mathbf{0} \leqslant \boldsymbol{\sigma} - \boldsymbol{\alpha} \quad \Longrightarrow \quad \boldsymbol{\alpha} \leqslant \boldsymbol{\sigma}$$

Veamos que cualquier subconjunto no vacío $A \subset \mathbb{N}^n$ posee mínimo para la relación $\leqslant$. Por la Proposición 1.15, para la relación $\ll$ si $A \subset \mathbb{N}^n$ es no vacío posee un conjunto finito de minimales $G = \{\boldsymbol{\alpha}(1), \boldsymbol{\alpha}(2), \ldots, \boldsymbol{\alpha}(s)\} \subset A$. Dado que nuestra relación de orden $\leqslant$ es de orden total, permutando índices si fuera necesario, podemos escribir $\boldsymbol{\alpha}(1) \leqslant \boldsymbol{\alpha}(2) \leqslant \cdots \leqslant \boldsymbol{\alpha}(s)$. Así, el elemento $\boldsymbol{\alpha}(1)$ es el mínimo de $(A, \leqslant)$. □

Observación 1.20. El Corolario 1.19 permite demostrar que un orden $\leqslant$ en $\mathbb{N}^n$ es monomial si, y sólo si, verifica las siguientes tres propiedades:

(m_1) $\leqslant$ es de orden total,
(m_2) $\leqslant$ es compatible con la suma y,
(m_3) para todo $\boldsymbol{\alpha} \in \mathbb{N}^n$, $\boldsymbol{\alpha} \geqslant \mathbf{0} = (0, \ldots, 0)$.

Ejemplos de órdenes monomiales: Es sencillo demostrar que los siguientes órdenes son monomiales comprobando las condiciones m_1, m_2, y m_3.

- **Orden Lexicográfico:** Dados $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathbb{N}^n$, diremos que $\boldsymbol{\alpha} >_{\text{lex}} \boldsymbol{\sigma}$ si, en el vector $\boldsymbol{\alpha} - \boldsymbol{\beta} \in \mathbb{Z}^n$ la primera entrada no nula empezando por la izquierda es positiva. Escribiremos $\boldsymbol{x}^{\boldsymbol{\alpha}} >_{\text{lex}} \boldsymbol{x}^{\boldsymbol{\beta}}$ si $\boldsymbol{\alpha} >_{\text{lex}} \boldsymbol{\beta}$.

  Notación: Dado $\boldsymbol{\alpha} \in \mathbb{N}^n$, denotaremos $|\boldsymbol{\alpha}| = \sum_{i=1}^{n} \alpha_i$.

- **Orden graduado lexicográfico:** Dados $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathbb{N}^n$,

$$\boldsymbol{\alpha} >_{\text{grlex}} \boldsymbol{\beta} \qquad :\Longleftrightarrow \qquad |\boldsymbol{\alpha}| > |\boldsymbol{\beta}| \qquad \text{o} \qquad |\boldsymbol{\alpha}| = |\boldsymbol{\beta}| \;\; \text{y} \;\; \boldsymbol{\alpha} >_{\text{lex}} \boldsymbol{\beta}$$

- **Orden graduado lexicográfico inverso:** Sean α y $\beta \in \mathbb{N}^n$. Decimos que $\boldsymbol{\alpha} >_{\text{grevlex}} \boldsymbol{\beta}$ si $|\boldsymbol{\alpha}| > |\boldsymbol{\beta}|$, o si $|\boldsymbol{\alpha}| = |\boldsymbol{\beta}|$ y la primera entrada no nula de $\boldsymbol{\alpha} - \boldsymbol{\beta} \in \mathbb{Z}^n$ empezando por la derecha es negativa.

Ejemplo 1.21. Aquí vemos diferentes comparaciones entre ternas de $\mathbb{N}^3$:

$$\begin{array}{lll}
(1,0,0) >_{\text{lex}} (0,7,6) & (3,2,6) >_{\text{lex}} (3,2,1) & (2,1,0) >_{\text{lex}} (1,7,3) \\
(5,4,3) >_{\text{grevlex}} (6,2,4) & (6,2,4) >_{\text{grlex}} (5,4,3) & (1,7,1) >_{\text{grlex}} (4,2,2) \\
(2,5,4) >_{\text{grlex}} (0,6,5) & (0,6,5) >_{\text{grevlex}} (2,5,4) & (4,1,1) >_{\text{lex}} (1,4,4)
\end{array}$$

Observación 1.22. Las variables $x_1, \ldots, x_n$ quedan ordenadas de igual forma para cualquiera de estos tres órdenes; si $>$ denota uno de los órdenes $>_{\text{lex}}$, $>_{\text{grlex}}$ o $>_{\text{grevlex}}$:

$$x_1 > x_2 > \cdots > x_n.$$

Si fijamos un orden monomial en el conjunto de los exponentes $\mathbb{N}^n$, dado un polinomio $f = \sum_{\boldsymbol{\alpha}} a_{\boldsymbol{\alpha}} \boldsymbol{x}^{\boldsymbol{\alpha}} \in K[x_1, \ldots, x_n]$ podemos ordenar sin ambigüedad los monomios de f respecto a dicha ordenación.

Ejemplo 1.23. Para fijar ideas, vamos a comparar como quedan ordenados los monomios de un polinomio según los diferentes órdenes monomiales que hemos visto hasta ahora. Sea $f = 7x^2y^2z + 3z^4 - 5x^3 + 2x^2yz^2 \in K[x, y, z]$. Sus monomios se ordenarían como sigue:

- Respecto a $>_{\text{lex}}$: $f = -5x^3 + 7x^2y^2z + 2x^2yz^2 + 3z^4$;
- Respecto a $>_{\text{grlex}}$: $f = 7x^2y^2z + 2x^2yz^2 + 3z^4 - 5x^3$;
- Respecto a $>_{\text{grevlex}}$: $f = 2x^2yz^2 + 7x^2y^2z + 3z^4 - 5x^3$.

Definición 1.24. Fijemos un orden monomial.

Dado polinomio no nulo $f = \sum_{\boldsymbol{\alpha}} a_{\boldsymbol{\alpha}} \boldsymbol{x}^{\boldsymbol{\alpha}} \in K[x_1, \ldots, x_n]$ se definen los siguientes elementos destacados del polinomio:

- El *multigrado* o *grado de* f: $\text{MGRAD}(f) := \text{máx}\{\boldsymbol{\alpha} \in \mathbb{N}^n / a_{\boldsymbol{\alpha}} \neq 0\}$;
- El *coeficiente principal de* f: $\text{LC}(f) := a_{\text{MGRAD}(f)}$;
- El *monomio principal de* f: $\text{LM}(f) := x^{\text{MGRAD}(f)}$;
- El *término principal de* f: $\text{LT}(f) := \text{LC}(f) \cdot \text{LM}(f) = a_{\text{MGRAD}(f)} \cdot x^{\text{MGRAD}(f)}$.

Ejemplo 1.25. De nuevo, para fijar ideas, vamos a ver quienes son los diferentes elementos destacados del polinomio f del ejemplo 1.23 según los órdenes monomiales que hemos introducido:

- Respecto a $>_{\text{lex}}$: $\text{LC}(f) = -5$, $\text{LM}(f) = x^3$, $\text{LT}(f) = -5x^3$;
- Respecto a $>_{\text{grlex}}$: $\text{LC}(f) = 7$, $\text{LM}(f) = x^2y^2z$, $\text{LT}(f) = 7x^2y^2z$;
- Respecto a $>_{\text{grevlex}}$: $\text{LC}(f) = 2$, $\text{LM}(f) = x^2yz^2$, $\text{LT}(f) = 2x^2yz^2$.

La demostración del siguiente lema es inmediata:

Lema 1.26. *Dados* $f, g \in K[x_1, \ldots, x_n]$ *polinomios no nulos:*

$$\text{MGRAD}(f \cdot g) = \text{MGRAD}(f) + \text{MGRAD}(g);$$
$$f + g \neq 0 \Rightarrow \text{MGRAD}(f + g) \leqslant \text{máx}\{\text{MGRAD}(f), \text{MGRAD}(g)\}.$$

1.4. Algoritmo de división en $\mathbf{K[x_1, \ldots, x_n]}$

Fijado un orden monomial $>$ en los exponentes $\mathbb{N}^n$. Una vez determinado el orden de los monomios de un polinomio no nulo, el siguiente paso es establecer un algoritmo de división que involucre varios divisores. Dado un polinomio $f \in K[\boldsymbol{x}]$, la idea de "dividir" f por una familia de polinomios $f_1, \ldots, f_s \in K[\boldsymbol{x}]$ consiste en expresar f en la forma $f = h_1 f_1 + \ldots + h_s f_s + r$, para ciertos polinomios $h_1, \ldots, h_s, r \in K[\boldsymbol{x}]$, de tal manera que r sea un "resto" que no se pueda simplificar utilizando los términos principales de los polinomios $f_1, \ldots, f_s$.

En el caso del anillo de polinomios en una variable $K[x]$ y un divisor f_1 bastaba exigir como condición para finalizar el algoritmo que $r = 0$, o que siendo $r \neq 0$ su grado fuese menor que el grado del divisor.

En el caso general la idea básica es cancelar el término principal de f multiplicando algún f_i por un monomio apropiado y restándolos, para a continuación repetir el proceso con el polinomio resultante de dicha operación, hasta que este proceso no se pueda repetir más. Para ver cómo proceder, empezaremos con un ejemplo:

Ejemplo 1.27. Consideremos el orden monomial lexicográfico, con $x > y$. Vamos a "dividir" $f = xy^2 + x$ por $f_1 = xy + 1$ y $f_2 = x + 1$:
Multiplicamos $f_1 \cdot y$ y se lo restamos a f:

$(xy^2 + x) - [(xy + 1) \cdot y] = x - y.$

Como xy no divide a x, pasamos a f_2: Multiplicamos $f_2 \cdot 1$ y se lo restamos al resultado anterior:

$x - y - [(x + 1) \cdot 1] = -y - 1.$

Como x no divide a y, hemos acabado y $r = -y - 1$. Concluímos:

$f = xy^2 + 1 = (xy + 1) \cdot y + (x + 1) \cdot 1 + (-y - 1) = f_1 \cdot a_1 + f_2 \cdot a_2 + r.$

Observamos que el resto obtenido, $r = -y-1$, no es divisible por el término principal de ninguno de los divisores. ¿Es esta condición la adecuada para poder definir correctamente el algoritmo?

Teorema 1.28 (Algoritmo de la división en $K[x_1, \ldots, x_n]$)**.** *Sea $F = (f_1, \ldots, f_s)$ una s-tupla ordenada de polinomios de $K[\boldsymbol{x}] = K[x_1, \ldots, x_n]$ y fijemos un orden monomial $(\mathbb{N}^n, \geqslant)$. Cada polinomio $f \in K[\boldsymbol{x}]$ se puede escribir de la siguiente forma:*

$$f = h_1 f_1 + \cdots + h_s f_s + r,$$

con $h_i, r \in K[x_1, \ldots, x_n]$, tales que $r = 0$ o r es una combinación K-lineal de monomios, ninguno de los cuales es divisible por ninguno de los $\text{LT}(f_i)$. Además, si $h_i f_i \neq 0$, entonces

$$\text{MGRAD}(f) \geqslant \text{MGRAD}(h_i f_i).$$

Nos referiremos a r como resto *de la división de f por la s-tupla ordenada $F = (f_1, \ldots, f_s)$, y escribiremos $r = \overline{f}^F$.*

Demostración. Demostraremos la existencia tanto de los coeficientes h_i como del resto r explicitando un algoritmo para hallarlos, y viendo que dicho algoritmo concluye en un número finito de pasos.

Input: $f_1, \ldots, f_s, f$
Output: $h_1, \ldots, h_s, r$
  $h_1 := 0; \ldots; h_s := 0; r := 0$
  $p := f$
  WHILE $p \neq 0$ DO
    $i := 1$
    divisionoccurred:=false
    WHILE $i \leqslant s$ AND divisionoccurred=false DO
      IF $\text{LT}(f_i)$ divides $\text{LT}(p)$ THEN
        $h_i := h_i + \text{LT}(p)/\text{LT}(f_i)$
        $p := p - (\text{LT}(p)/\text{LT}(f_i))f_i$
        divisionoccurred:= true
      ELSE
        $i := i + 1$
    IF divisionoccurred=false THEN
      $r := r + \text{LT}(p)$
      $p := p - \text{LT}(p)$

Donde la variable p representa el dividendo, que puede ser distinto en cada iteración del algoritmo. La variable lógica divisionoccurred nos indica cuando el término $\text{LT}(f_i)$ divide al término principal del dividendo p.

Para probar que dicho algoritmo funciona, observemos que la igualdad

$$f = h_1 f_1 + \ldots + h_s f_s + p + r \tag{1.4}$$

se mantiene en cada iteración. En cada iteración del bucle principal WHILE...DO se da una y sólo una de las siguientes situaciones: O bien $\text{LT}(f_i)$ divide a $\text{LT}(p)$, en cuyo caso se procede de forma análoga al algoritmo en una variable, o bien $\text{LT}(f_i)$ no divide a $\text{LT}(p)$, en cuyo caso $\text{LT}(p)$ se añade al resto. En el caso de que $\text{LT}(f_i)$ divida a $\text{LT}(p)$, se produce el siguiente cambio:

$$h_i f_i + p = (h_i + \text{LT}(p)/\text{LT}(f_i))f_i + (p - \text{LT}(p)/\text{LT}(f_i))f_i,$$

mientras que en el otro caso, tenemos que

$$p + r = (p - \text{LT}(p)) + (r + \text{LT}(p)),$$

con lo cual la igualdad (1.4) se mantiene. Nos falta probar que el algoritmo termina, es decir, que llega un momento en el cual $p = 0$. Para ver esto observemos lo que le ocurre a p en cada iteración: Si $\text{LT}(f_i)$ divide a $\text{LT}(p)$, redefinimos p como $p - (\text{LT}(p)/\text{LT}(f_i))f_i$, mientras que en el otro caso, redefinimos p como $p - \text{LT}(p)$. En ambas situaciones se produce una resta de dos polinomios que tienen el mismo término principal, y por tanto, se cancelan y el multigrado de p disminuye. Si el algoritmo no terminase en un número finito de pasos, obtendríamos una sucesión infinita estrictamente decreciente de multigrados, y esto contradice el hecho de que el orden elegido sea un orden monomial. □

Observación 1.29. El problema es que este algoritmo no conserva las buenas propiedades de su versión en 1 variable, como la unicidad del resto: Ni los coeficientes $h_1, \ldots, h_s$ ni el "resto" r quedan determinados de forma única por el dividendo f y el "divisor" $F = (f_1, \ldots, f_s)$. Podemos observar este hecho en el siguiente ejemplo:

Ejemplo 1.30. Sea $f = x^2y + xy + y$ un polinomio. Vamos a dividir f por $f_1 = xy - 1$ y por $f_2 = x - 1$ considerando en $K[x, y]$ el orden lexicográfico, con $x > y$.

(I) Consideremos $F_{12} = (f_1, f_2)$:

Dado que $\text{LT}(f)$ es divisible por $\text{LT}(f_1)$, restamos a f el producto $f_1 \cdot x$:

$(x^2y + xy + y) - [(xy - 1) \cdot x] = xy - x + y$

Como xy es divisible por $\text{LT}(f_1)$, restamos a $xy - x + y$ el producto $f_1 \cdot 1$:

$(xy - x + y) - [(xy - 1) \cdot 1] = -x + y - 1$

Como x no es divisible por $\text{LT}(f_1)$, pasamos al polinomio f_2. Le restamos a $-x + y - 1$ el producto $f_2 \cdot (-1)$

$(-x + y - 1) - [(x - 1) \cdot (-1)] = y - 2$

De esta forma, $f = (x + 1) \cdot f_1 - f_2 + y - 2$, y el resto es: $r = y - 2$.

(II) Consideremos ahora $F_{21} = (f_2, f_1)$:

Dado que $\text{LT}(f)$ es divisible por $\text{LT}(f_2)$, restamos a f el producto $f_2 \cdot xy$

$(x^2y + xy + y) - [(x - 1) \cdot xy] = 2xy + y$

Como xy es divisible por $\text{LT}(f_2)$, restamos a $2xy + y$ el producto $f_2 \cdot 2y$

$(2xy + y) - [(x - 1) \cdot 2y] = y + 2y = 3y$

Y como y no es divisible por $\text{LT}(f_1)$ ni por $\text{LT}(f_2)$, obtenemos que $f = (xy + 2y) \cdot f_2 + 3y$, y en este caso el resto es: $r = 3y$.

Observación 1.31. Que el resto quede determinado o no de forma única es relevante para determinar si un polinomio dado pertenece a un ideal. Si al dividir f por $F = (f_1, \ldots, f_s)$

resulta $r = 0$, entonces $f \in \langle f_1, \ldots, f_s \rangle$. Pero que se obtenga un resto $r \neq 0$ al aplicar el algoritmo de la división para una s-upla $F = (f_1, \ldots, f_s)$ no nos permite concluir que $f \notin \langle f_1, \ldots, f_s \rangle$, ya que podríamos obtener resto cero respecto a una s-upla F' obtenida cambiando el orden de la colección del divisores, como hemos visto en el ejemplo.

Podríamos pensar si cambiando el conjunto de generadores $\{f_1, \ldots, f_s\}$ de un ideal I sería posible arreglar el problema de la unicidad del resto en el algoritmo de la división ¿Es posible encontrar un conjunto de generadores $\{f_1, \ldots, f_s\}$ del ideal I para el que resto obtenido al aplicar el algoritmo de la división no dependa del orden elegido en el conjunto de divisores $f_1, \ldots, f_s$?

1.5. Definición y existencia de la base de Groebner: Teorema de la Base de Hilbert.

Una vez seleccionado un orden monomial, cada polinomio de $K[\boldsymbol{x}]$ tiene un único término principal. Dado $I \subset K[\boldsymbol{x}] = K[x_1, \ldots, x_n]$ un ideal,

- Denotamos por $\text{LT}(I)$ el conjunto de los términos principales de elementos de I, $\text{LT}(I) = \{\text{LT}(f) \ / \ f \in I - \{0\}\}$.
- Denotamos por $\langle \text{LT}(I) \rangle$ el ideal monomial generado por los elementos de $\text{LT}(I)$.

Si $I = \langle f_1, \ldots, f_s \rangle$, entonces $\langle \text{LT}(I) \rangle$ y $\langle \text{LT}(f_1), \ldots, \text{LT}(f_s) \rangle$ pueden no ser iguales. La única inclusión que está garantizada es $\langle \text{LT}(I) \rangle \supset \langle \text{LT}(f_1), \ldots, \text{LT}(f_s) \rangle$. El siguiente ejemplo nos muestra que no siempre se tiene la igualdad.

Ejemplo 1.32. Sea $I = \langle f_1, f_2 \rangle$, con $f_1 = x^3 - 2xy$, $f_2 = x^2y - 2y^2 + x$ y consideremos la relación de orden $>_{\text{grlex}}$:

$x \cdot (x^2y - 2y^2 + x) - y \cdot (x^3 - 2xy) = x^2 \Longrightarrow x^2 \in I \Longrightarrow x^2 \in \langle \text{LT}(I) \rangle$

x^2 no es divisible por $\text{LT}(f_1) = x^3$ ni por $\text{LT}(f_2) = x^2y \Longrightarrow x^2 \notin \langle \text{LT}(f_1), \text{LT}(f_2) \rangle$

Lema 1.33. *Dado un orden monomial, si $I \subset K[\boldsymbol{x}]$ es un ideal, existen $g_1, \ldots, g_t \in I$ tales que $\langle \text{LT}(I) \rangle = \langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle$.*

Demostración. Como $\langle \text{LT}(I) \rangle$ es un ideal monomial es finitamente generado, por el Lema de Dickson (Corolario 1.15). Sea $x^{\boldsymbol{\alpha}(1)}, \ldots, x^{\boldsymbol{\alpha}(t)}$ un sistema de generadores de $\langle \text{LT}(I) \rangle$. Por el Lema 1.13, podemos suponer que cada monomio mónico $x^{\boldsymbol{\alpha}(i)}$ es de la forma $x^{\boldsymbol{\alpha}(i)} = \text{LM}(g_i)$ para cierto polinomio $g_i \in I$. □

Teorema 1.34. *Sea $I \subset K[x_1, \ldots, x_n]$ un ideal y $g_1, \ldots, g_t \in I$ elementos no nulos. Para cualquier orden monomial se verifica:*

$$\langle \text{LT}(I) \rangle = \langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle \qquad \Longrightarrow \qquad I = \langle g_1, \ldots, g_t \rangle.$$

Demostración. Fijemos un orden monomial. Trivialmente $\langle g_1, \ldots, g_t \rangle \subset I$, veamos el otro contenido. Sea $f \in I$, aplicando a f el algoritmo de la división por $g_1, \ldots, g_t$ se obtiene una expresión:

$$f = h_1 g_1 + \ldots + h_t g_t + r \qquad (h_1, \ldots, h_t, r \in K[\boldsymbol{x}])$$

donde $r = 0$ o $r \neq 0$ y ninguno de sus monomios es divisible por ninguno de los $\text{LT}(g_i)$. Si $r = 0$ entonces habríamos concluido que $f \in \langle g_1, \ldots, g_t \rangle$. Si $r \neq 0$, despejando r de la ecuación anterior se tiene que $r = f - (h_1 g_1 + \ldots + h_t g_t)$. De aquí deducimos que $r \in I$, y por tanto $\text{LT}(r) \in \langle \text{LT}(I) \rangle = \langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle$. Por el Lemma 1.13, el término principal de r es

divisible por el término principal de algún g_i, lo cual es no es posible por el algoritmo de la división. Entonces necesariamente $r = 0$, y por tanto $f = h_1g_1 + \ldots + h_tg_t \in \langle g_1, \ldots, g_t \rangle$. □

Observación 1.35. Fijado un orden monomial en $\mathbb{N}^n$, según el Lema 1.33, para cualquier ideal no nulo $I \subset K[\boldsymbol{x}]$ existe una una colección de elementos $g_1, \ldots, g_t \in I$ no nulos tales que $\langle \text{LT}(I) \rangle = \langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle$; y por el Teorema 1.34 la colección de elementos $g_1, \ldots, g_t$ es un sistema de generadores del ideal I. Este tipo de sistemas de generadores son un elemento clave en el buen funcionamiento del algoritmo de división, y es la motivación de la siguiente definición:

Definición 1.36. Fijado un orden monomial, se dice que un conjunto de generadores $g_1, \ldots, g_t \in I - \{0\}$ de un ideal $I \subset K[\boldsymbol{x}]$ es una *base de Groebner* de I si

$$\langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle = \langle \text{LT}(I) \rangle.$$

Como consecuencia de los resultados anteriores:

Corolario 1.37. *Fijado un orden monomial en $K[\boldsymbol{x}]$ y un ideal $I \subset K[\boldsymbol{x}]$ no nulo. Entonces I posee al menos una base de Groebner. Además, toda base de Groebner de I es un conjunto de generadores de I.*

Demostración. El argumento de la Observación 1.35 demuestra este resultado. □

Corolario 1.38 (Teorema de la Base de Hilbert)**.** *Todo ideal $I \subset K[x_1, \ldots, x_n]$ tiene un conjunto finito de generadores: existen $g_1, \ldots, g_t \in I$ tales que $I = \langle g_1, \ldots, g_t \rangle$.*

Demostración. Elegido un orden monomial, se deduce del Corolario 1.37. □

Observación 1.39. Fijado un orden monomial, un ideal $I \subset K[\boldsymbol{x}]$ no posee una única base de Groebner. Además, que un conjunto de generadores de un ideal $I \subset K[\boldsymbol{x}]$ sea o no una base de Groebner depende del orden monomial considerado.

Observación 1.40. Como primera aplicación del Teorema de la Base de Hilbert (Corolario 1.38), tenemos las siguientes consecuencias:

- $K[x_1, \ldots, x_n]$ es un anillo noetheriano, es decir, se verifica la condición de cadena ascendente: Si $I_1 \subset I_2 \subset I_3 \subset \ldots$ es una cadena ascendente de ideales en $K[x_1, \ldots, x_n]$, existe un $N \geqslant 1$ tal que $I_N = I_{N+1} = I_{N+2} = \ldots$
- Además, recordemos que una variedad algebraica se definía como el conjunto de puntos de K^n que eran solución de un sistema arbitrario de ecuaciones polinómicas. Gracias a este teorema, el problema de hallar los puntos de una variedad algebraica se reduce a resolver un sistema con un número finito de ecuaciones polinómicas.

1.6. Propiedades de las bases de Groebner.

Una de las propiedades más importantes de las bases de Groebner, y que de hecho motivó su definición, es la siguiente proposición, que establece que usando como divisores los elementos de una base de Groebner de un ideal, el resto del algoritmo de la división de un polinomio dado no depende del orden elegido para los divisores.

Proposición 1.41. *Fijemos un orden monomial. Sea $G = \{g_1, \ldots, g_t\}$ una base de Groebner de un ideal $I \subset K[\boldsymbol{x}]$ y sea $f \in K[\boldsymbol{x}]$ un polinomio. Entonces existen un único par de polinomios r, $g \in K[\boldsymbol{x}]$ que verifican las siguientes propiedades:*

(1) $g \in I$, y es tal que $f = g + r$, y

(2) si $r \neq 0$, ningún monomio de r es divisible por ninguno de los $\mathrm{LT}(g_i)$, $i \in \{1, \ldots, t\}$.

Demostración. La existencia de la expresión $f = g + r$ con $g \in I$ y $r \in K[\boldsymbol{x}]$ en las condiciones del enunciado viene garantizada por el algoritmo de la división en $K[\boldsymbol{x}]$. Veamos la unicidad: supongamos que $f = g+r = g'+r'$ son dos descomposiciones del tipo indicado en el enunciado para f. Entonces $r' - r = g - g' \in I$. Si $r \neq r'$ entonces $r' - r \neq 0$ y $\mathrm{LT}(r' - r) \in \langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$, y de aquí deducimos que $\mathrm{LT}(r' - r)$ es divisible por alguno de los monomios $\mathrm{LT}(g_i)$. Lo cual es una contradicción ya que $\mathrm{LT}(r' - r)$ es un múltiplo de uno de los monomios de r o r' y ninguno es divisible por ninguno de los $\mathrm{LT}(g_i)$, $i \in \{1, \ldots, t\}$. Entonces necesariamente $r = r'$. □

Notación 1.42. Fijado un orden monomial. Sea $G = \{g_1, \ldots, g_t\}$ una base de Groebner del ideal $I \subset K[\boldsymbol{x}]$, $f \in K[\boldsymbol{x}]$ un polinomio y $f = g + r$ es una descomposición verificando las condiciones de la proposición anterior. El polinomio r se denomina, por razones obvias, *resto* de la división de f por la base de Groebner G. En adelante escribiremos $r = \overline{f}^G$.

Corolario 1.43. *Sea $G = \{g_1, \ldots, g_t\}$ una base de Groebner del ideal $I \subset K[\boldsymbol{x}]$ para un orden monomial. Dado $f \in K[\boldsymbol{x}]$, entonces $f \in I$ si, y sólo si, $\overline{f}^G = 0$.*

Demostración. Trivialmente, si $\overline{f}^G = 0, f \in I$. Recíprocamente, por el algoritmo de la división, dado un polinomio $f \in K[\boldsymbol{x}]$, podemos escribir f como: $f = h_1 g_1 + \cdots h_t g_t + r$, con $h_1, \ldots, h_t, r \in I$ donde $r = \overline{f}^G$. Si $f \in I$, de las expresiones $f = g + r$ y $f = f + 0$, se deduce que $r = 0$ (Proposición 1.41). □

Observación 1.44. Queda completamente resuelto el *problema de determinar si un polinomio dado pertenece a un ideal*: Basta fijar un orden monomial, buscar una base de Groebner del ideal y ejecutar el algoritmo de la división para saber si un polinomio pertenece o no a dicho ideal.

1.6.1. Criterio para determinar bases de Groebner.

Fijemos una ordenación de monomios en $K[\boldsymbol{x}] = K[x_1, \ldots, x_n]$.

Definición 1.45. Sean $f, g \in K[\boldsymbol{x}]$ polinomios no nulos, de grados $\boldsymbol{\alpha} = \text{MGRAD}(f)$ y $\boldsymbol{\beta} = \text{MGRAD}(g)$; y sea $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_n)$, con $\gamma_i = \text{máx}\{\alpha_i, \beta_i\}$. Decimos que $\boldsymbol{x}^{\boldsymbol{\gamma}}$ es el mínimo común múltiplo de $\text{LM}(f)$ y $\text{LM}(g)$:

$$\boldsymbol{x}^{\boldsymbol{\gamma}} = \text{lcm}(\text{LM}(f), \text{LM}(g)).$$

Definición 1.46. La *sizigia* de f y g, que denotaremos por $\text{S}(f, g)$, es el polinomio

$$\text{S}(f, g) = \frac{\boldsymbol{x}^{\boldsymbol{\gamma}}}{\text{LT}(f)} \cdot f - \frac{\boldsymbol{x}^{\boldsymbol{\gamma}}}{\text{LT}(g)} \cdot g$$

Observación 1.47. Las sizigias están diseñadas para producir cancelaciones en los términos principales de los polinomios. De hecho, el siguiente lema demuestra que toda cancelación de términos principales en una suma de polinomios puede efectuarse empleando sizigias.

Lema 1.48. *Supongamos que tenemos una suma de la forma*

$$h := \sum_{i=1}^{t} c_i \cdot \boldsymbol{x}^{\boldsymbol{\alpha}(i)} \cdot g_i,$$

donde los escalares $c_i \in K$, los polinomios $g_i \in K[\boldsymbol{x}]$ involucrados son no nulos y los sumandos tiene todos el mismo grado $\boldsymbol{\alpha}(i) + \text{MGRAD}(g_i) = \boldsymbol{\delta}$. Si $\text{MGRAD}(h) < \boldsymbol{\delta}$, entonces existen escalares $c_{jk} \in K$ tales que

$$\sum_{i=1}^{t} c_i \cdot \boldsymbol{x}^{\boldsymbol{\alpha}(i)} \cdot g_i = \sum_{j,k} c_{jk} \cdot \boldsymbol{x}^{\boldsymbol{\delta} - \boldsymbol{\gamma}(jk)} \cdot \text{S}(g_j, g_k),$$

donde $\boldsymbol{x}^{\boldsymbol{\gamma}(jk)} = \text{lcm}(\text{LM}(g_j), \text{LM}(g_k))$. Además, cada término $\boldsymbol{x}^{\boldsymbol{\delta} - \boldsymbol{\gamma}(jk)} \cdot \text{S}(g_j, g_k)$ no nulo tiene multigrado menor que $\boldsymbol{\delta}$.

Demostración. Sea $d_i = \text{LC}(g_i)$, de modo que $c_i d_i = \text{LC}(c_i \boldsymbol{x}^{\boldsymbol{\alpha}(i)} g_i)$. Dado que cada sumando $c_i \boldsymbol{x}^{\boldsymbol{\alpha}(i)} g_i$ tiene multigrado $\boldsymbol{\delta}$ y la suma tiene multigrado estrictamente menor, necesariamente $\sum_{i=1}^{t} c_i d_i = 0$.

Para cada $i \in \{1, \ldots, t\}$ sea $p_i \in K[\boldsymbol{x}]$ el polinomio mónico

$$p_i := \frac{\boldsymbol{x}^{\boldsymbol{\alpha}(i)} g_i}{d_i}.$$

Consideremos la suma telescópica

$$\begin{aligned} \sum_{i=1}^{t} c_i \boldsymbol{x}^{\boldsymbol{\alpha}(i)} g_i = \sum_{i=1}^{t} c_i d_i p_i &= c_1 d_1 (p_1 - p_2) + (c_1 d_1 + c_2 d_2)(p_2 - p_3) + \cdots \\ &\cdots + (c_1 d_1 + s + c_{t-1} d_{t-1})(p_{t-1} - p_t) + (c_1 d_1 + \ldots c_t d_t) p_t. \end{aligned}$$

Siendo $\boldsymbol{\beta}(i) := \text{MGRAD}(g_i)$, $\text{LT}(g_i) = d_i \boldsymbol{x}^{\boldsymbol{\beta}(i)}$, para cada i. Por hipótesis, tenemos que $\boldsymbol{\alpha}(i) + \boldsymbol{\beta}(i) = \boldsymbol{\delta}$, y entonces el monomio $\text{LM}(g_i) = \boldsymbol{x}^{\boldsymbol{\beta}(i)}$ divide a $\boldsymbol{x}^{\boldsymbol{\delta}}$. Consecuentemente, $\boldsymbol{x}^{\boldsymbol{\gamma}(jk)} = \text{lcm}(\text{LM}(g_j), \text{LM}(g_k))$ también divide a $\boldsymbol{x}^{\boldsymbol{\delta}}$. Por tanto, podemos escribir:

$$\begin{aligned} \boldsymbol{x}^{\boldsymbol{\delta}-\boldsymbol{\gamma}(jk)} \cdot \text{S}(g_j, g_k) &= \boldsymbol{x}^{\boldsymbol{\delta}-\boldsymbol{\gamma}(jk)} \cdot \left(\frac{\boldsymbol{x}^{\boldsymbol{\gamma}(jk)}}{\text{LT}(g_j)} g_j - \frac{\boldsymbol{x}^{\boldsymbol{\gamma}(jk)}}{\text{LT}(g_k)} g_k \right) \\ = \frac{\boldsymbol{x}^{\boldsymbol{\delta}}}{d_j \boldsymbol{x}^{\boldsymbol{\beta}(j)}} g_j - \frac{\boldsymbol{x}^{\boldsymbol{\delta}}}{d_k \boldsymbol{x}^{\boldsymbol{\beta}(k)}} g_k &= \frac{\boldsymbol{x}^{\boldsymbol{\alpha}(j)} g_j}{d_j} - \frac{\boldsymbol{x}^{\boldsymbol{\alpha}(k)} g_k}{d_k} = p_j - p_k; \end{aligned}$$

usando esta relación, y que $\sum_{i=1}^{t} c_i d_i = 0$, la suma telescópica anterior se escribirse

$$\begin{aligned} \sum_{i=1}^{t} c_i \cdot \boldsymbol{x}^{\boldsymbol{\alpha}(i)} \cdot g_i = c_1 d_1 \cdot \boldsymbol{x}^{\boldsymbol{\delta}-\boldsymbol{\gamma}(12)} \cdot \text{S}(g_1, g_2) + (c_1 d_1 + c_2 d_2) \cdot \boldsymbol{x}^{\boldsymbol{\delta}-\boldsymbol{\gamma}(23)} \cdot \text{S}(g_2, g_3) + \cdots \\ \cdots + (c_1 d_1 + \ldots + c_{t-1} d_{t-1}) \cdot \boldsymbol{x}^{\boldsymbol{\delta}-\boldsymbol{\gamma}(t-1,t)} \cdot \text{S}(g_{t-1}, g_t), \end{aligned}$$

que es una suma de la forma deseada. Como p_j y p_k tienen multigrado $\boldsymbol{\delta}$ y coeficiente principal 1, la diferencia $p_j - p_k$ tiene multigrado menor que $\boldsymbol{\delta}$. Esto permite concluír que $\boldsymbol{x}^{\boldsymbol{\delta}-\boldsymbol{\gamma}(jk)} \text{S}(g_j, g_k)$ también tiene multigrado menor que $\boldsymbol{\delta}$. □

Como hemos dicho anteriormente, este lema demuestra que toda cancelación puede llevarse a cabo utilizando sizigias. Para ver esto fijémonos en la ecuación

$$\sum_{i=1}^{t} c_i \boldsymbol{x}^{\boldsymbol{\alpha}(i)} g_i = \sum_{j,k} c_{jk} x^{\boldsymbol{\delta}-\boldsymbol{\gamma}(jk)} \text{S}(g_j, g_k),$$

y analicemos cuándo ocurre la cancelación de términos principales: en el lado izquierdo de la igualdad, cada sumando $c_i x^{\boldsymbol{\alpha}(i)} g_i$ tiene multigrado $\boldsymbol{\delta}$, por tanto la cancelación sólo ocurre al sumar los términos. Sin embargo, en el lado derecho de la igualdad, cada sumando $x^{\delta-\gamma_{jk}} \text{S}(g_j, g_k)$ tiene multigrado menor que δ, y por lo tanto la cancelación ya se ha producido. Es decir, dada una suma de términos en los que el monomio de mayor grado se cancela, siempre podemos reescribirla como una suma de monomios de grado menor empleando sizigias.

Usando las sizigias y el Lema 1.48, se demuestra el siguiente criterio para determinar cuando un conjunto de generadores de un ideal es una base de Groebner:

Teorema 1.49. *Sea $I = \langle g_1, \ldots, g_t \rangle \subset K[\boldsymbol{x}]$ un ideal. El conjunto $G = \{g_1, \ldots, g_t\}$ es una base de Groebner de I si, y sólo si, $\overline{\text{S}(g_i, g_j)}^{G} = 0$ para cualesquiera $i, j \in \{1, \ldots, t\}$.*

Demostración. Si G es una base de Groebner, como $\text{S}(g_i, g_j) \in I$, su resto al dividirlo por los elementos de G será cero en virtud del Corolario 1.43. Recíprocamente, si el resto de dividir todas las sizigias $\text{S}(g_i, g_j)$ por G es cero, veamos que para cualquier polinomio no

nulo $f \in I$ se verifica que $\text{LT}(f) \in \langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle$. Si $f \in I = \langle g_1, \ldots, g_t \rangle$ es no nulo, existirán polinomios $h_i \in K[x_1, \ldots, x_n]$ tales que

$$f = \sum_{i=1}^{t} h_i g_i. \tag{1.5}$$

Obsérvese que

$$\text{MGRAD}(f) \leqslant \text{máx}\{\text{MGRAD}(h_i g_i); 1 \leq i \leq t,\ h_i g_i \neq 0\}. \tag{1.6}$$

Dada una expresión del tipo (1.5) para f, denotemos $\boldsymbol{\mu}(i) = \text{MGRAD}(h_i g_i)$, siendo $h_i g_i \neq 0$. Sea $A = \{\boldsymbol{\mu}(i); 1 \leq i \leq t,\ h_i g_i \neq 0\}$ y $\boldsymbol{\delta} = \text{máx}\, A$, entonces la desigualdad (1.6) se puede reescribir como: $\text{MGRAD}(f) \leqslant \boldsymbol{\delta}$. Consideramos para f todas las posibles expresiones del tipo (1.5). Para cada una de estas expresiones, podemos obtener un $\boldsymbol{\delta}$ distinto, pero dado que el orden monomial es un buen orden, podemos elegir una expresión de la forma (1.5) para f de forma que $\boldsymbol{\delta}$ sea de grado mínimo.

Si $\text{MGRAD}(f) = \boldsymbol{\delta}$, es decir, $\text{MGRAD}(f) = \text{MGRAD}(h_{i_0} g_{i_0})$ para algún $i_0 \in \{1, \ldots, t\}$ entonces $\text{LT}(g_{i_0})$ divide a $\text{LT}(f)$, por tanto $\text{LT}(f) \in \langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle$. Habríamos concluido la demostración. Veamos que el otro caso $\text{MGRAD}(f) < \boldsymbol{\delta}$ no es posible por reducción al absurdo:

Supongamos que $\text{MGRAD}(f) < \boldsymbol{\delta}$ y escribamos f de la forma siguiente:

$$f = \sum_{\boldsymbol{\mu}(i) = \boldsymbol{\delta}} h_i g_i \ + \sum_{\boldsymbol{\mu}(i) < \boldsymbol{\delta}} h_i g_i.$$

Si separamos los términos principales de los polinomios h_i, podemos reescribir f de la siguiente forma:

$$f = \left(\sum_{\boldsymbol{\mu}(i) = \boldsymbol{\delta}} \text{LT}(h_i) g_i \right) + \left(\sum_{\boldsymbol{\mu}(i) = \boldsymbol{\delta}} (h_i - \text{LT}(h_i)) g_i \ + \sum_{\boldsymbol{\mu}(i) < \boldsymbol{\delta}} h_i g_i \right) \tag{1.7}$$

El sumando de la derecha es a su vez suma de términos de multigrado menor que $< \boldsymbol{\delta}$. Por tanto, la hipótesis $\text{MGRAD}(f) < \boldsymbol{\delta}$ equivale a que el sumando de la izquierda tenga multigrado $< \boldsymbol{\delta}$.

Para cada i tal que $\boldsymbol{\mu}(i) = \boldsymbol{\delta}$, sea $\text{LT}(h_i) = c_i \boldsymbol{x}^{\boldsymbol{\alpha}(i)}$. Entonces, el primer sumando en (1.7) se escribe de la forma

$$\sum_{\boldsymbol{\mu}(i) = \boldsymbol{\delta}} \text{LT}(h_i) g_i = \sum_{\boldsymbol{\mu}(i) = \boldsymbol{\delta}} c_i \boldsymbol{x}^{\boldsymbol{\alpha}(i)} g_i.$$

Una vez obtenida esta expresión, estamos en las condiciones del enunciado del Lema 1.48, pues $\text{MGRAD}(c_i \boldsymbol{x}^{\boldsymbol{\alpha}(i)} g_i) = \boldsymbol{\delta}$ y la suma tiene grado $< \boldsymbol{\delta}$. Por el Lema 1.48, tenemos que:

$$\sum_{\boldsymbol{\mu}(i) = \delta} \text{LT}(h_i) g_i = \sum_{\boldsymbol{\mu}(i) = \boldsymbol{\delta}} c_i \boldsymbol{x}^{\boldsymbol{\alpha}(i)} g_i = \sum_{j,k} c_{jk} \cdot \boldsymbol{x}^{\boldsymbol{\delta} - \boldsymbol{\gamma}(jk)} \cdot \text{S}(g_j, g_k), \tag{1.8}$$

donde $c_{jk} \in K$ y $\boldsymbol{x}^{\boldsymbol{\gamma}(jk)} = \operatorname{lcm}(\operatorname{LM}(g_j), \operatorname{LM}(g_k))$.

Por hipótesis, aplicando el algoritmo de la división el resto de dividir $\mathrm{S}(g_j, g_k)$ por $g_1, \ldots, g_t$ es cero, por tanto existen polinomios $a_{ijk} \in K[\boldsymbol{x}]$ tales que

$$\mathrm{S}(g_j, g_k) = \sum_{i=1}^{t} a_{ijk} \cdot g_i,$$

y, por el algoritmo de la división, para los sumandos no nulos se verifica la acotación

$$\operatorname{MGRAD}(a_{ijk} g_i) \leqslant \operatorname{MGRAD}(\mathrm{S}(g_j, g_k)). \tag{1.9}$$

Multiplicando $\mathrm{S}(g_j, g_k)$ por $x^{\boldsymbol{\delta}-\boldsymbol{\gamma}(jk)}$ obtenemos la expresión

$$\boldsymbol{x}^{\delta-\boldsymbol{\gamma}(jk)} \cdot \mathrm{S}(g_j, g_k) = \sum_{i=1}^{t} b_{ijk} g_i, \tag{1.10}$$

con $b_{ijk} := \boldsymbol{x}^{\boldsymbol{\delta}-\boldsymbol{\gamma}(jk)} a_{ijk}$. El Lema 1.48 y la desigualdad (1.9) nos dicen que

$$\operatorname{MGRAD}(b_{ijk} g_i) \leqslant \operatorname{MGRAD}(\boldsymbol{x}^{\boldsymbol{\delta}-\boldsymbol{\gamma}(jk)} \cdot \mathrm{S}(g_j, g_k)) < \boldsymbol{\delta}, \tag{1.11}$$

siempre que los polinomios involucrados en la expresión sean no nulos. Si sustituimos la expresión (1.10) en la ecuación (1.8), se obtiene

$$\sum_{\boldsymbol{\mu}(i)=\boldsymbol{\delta}} \operatorname{LT}(h_i) g_i = \sum_{j,k} c_{jk} \left(\sum_{i=1}^{t} b_{ijk} g_i \right) = \sum_{i=1}^{t} \left(\sum_{j,k} c_{jk} b_{ijk} \right) g_i = \sum_{i=1}^{t} \widetilde{h}_i g_i, \tag{1.12}$$

siendo $\widetilde{h}_i := \sum_{j,k} c_{jk} b_{ijk}$. Si $\widetilde{h}_i g_i \neq 0$, de la ecuación (1.11) se sigue que $\operatorname{MGRAD}(\widetilde{h}_i g_i) < \boldsymbol{\delta}$ (ya que los c_{jk} son escalares). Finalmente, sustituyendo $\sum_{\boldsymbol{\mu}(i)=\boldsymbol{\delta}} \operatorname{LT}(h_i) g_i = \sum_{i=1}^{t} \widetilde{h}_i g_i$ en la ecuación (1.7), obtenemos la expresión para f:

$$f = \sum_{i=1}^{t} \widetilde{h}_i g_i \; + \sum_{\boldsymbol{\mu}(i)=\boldsymbol{\delta}} (h_i - \operatorname{LT}(h_i)) g_i \; + \sum_{\boldsymbol{\mu}(i)<\boldsymbol{\delta}} h_i g_i,$$

del tipo (1.5) en la que todos los sumandos tienen multigrado $< \boldsymbol{\delta}$. Esto contradice la minimalidad de $\boldsymbol{\delta}$, concluyendo que necesariamente $\operatorname{MGRAD}(f) = \boldsymbol{\delta}$. □

El Teorema 1.49 proporciona un algoritmo para comprobar si un conjunto dado de generadores de un ideal es una base de Groebner. Veamos un ejemplo muy básico de como realizar dicho algoritmo:

Ejemplo 1.50. Consideremos el ideal $I = \langle x - z^2, y - z^3 \rangle$.
Vamos a comprobar que el conjunto $G = \{x - z^2, y - z^3\}$ es una base de Groebner de I con el orden lexicográfico, con $x > y > z$.

Como en G solo hay 2 polinomios, la única sizigia que se puede construír con sus elementos es:

$$\mathrm{S}(x-z^2, y-z^3) = \frac{xy}{x}(x-z^2) - \frac{xy}{y}(y-z^3) = xz^3 - yz^2.$$

Ahora, si ejecutamos el algoritmo de la división para dividir este polinomio por G obtenemos:

$$\mathrm{S}(x-z^2, y-z^3) = xz^3 - yz^2 = z^3 \cdot (x-z^2) + (-z^2) \cdot (y-z^3) + 0.$$

Se tiene que el resto es cero, es decir: $\overline{S(x-z^2, y-z^3)}^G = 0$, y entonces en virtud del Teorema 1.49 podemos afirmar que G es una base de Groebner para el ideal I con el orden monomial elegido.

Sin embargo, G no es una base de Groebner de I si el orden considerado es el graduado lexicográfico, con $x > y > z$, ya que en este caso los monomios z^2 y z^3 son mayores que los monomios x e y respectivamente, y se producirían los siguientes resultados:

$$\mathrm{S}(-z^2+x, -z^3+y) = \frac{z^3}{z^2}(-z^2+x) - \frac{z^3}{z^3}(-z^3+y) = xz - y.$$

Dado que z^2 y z^3 no dividen ni a xz ni a y, el resultado al ejecutar el algoritmo de la división es:

$$\mathrm{S}(x-z^2, y-z^3) = 0 \cdot (-z^2+x) + 0 \cdot (-z^3+y) + xz - y$$

Es decir: $\overline{S(x-z^2, y-z^3)}^G = xz - y \neq 0$.

1.6.2. Construcción de una base de Groebner: Algoritmo de Buchberger.

Por el Corolario 1.37, tenemos garantizado que todo ideal $I \neq \{0\}, I \in K[x_1, \ldots, x_n]$ tiene al menos una base de Groebner. Ahora veremos un procedimiento para encontrar dicha base.

Teorema 1.51 (Algoritmo de Buchberger)**.** *Sea $I = \langle f_1, \ldots, f_s \rangle \neq 0$ un ideal de polinomios. Entonces una base de Groebner para I puede construírse en un número finito de pasos usando el siguiente algortimo:*

Input:= $F = (f_1, \ldots, f_s)$
Output:= $G = (g_1, \ldots, g_t), F \subset G$
  $G := F$
  REPEAT
    $G' := G$
    FOR cada par $\{p, q\}, p \neq q \in G'$ *DO*

$$T := \overline{\mathrm{S}(p,q)}^{G'}$$
$$IF\ \mathrm{S} \neq 0\ \ THEN\ G := G \cup \{T\}$$
$$UNTIL\ G := G'$$

Demostración. Primero comprobaremos que el conjunto G que hemos definido siempre está contenido en I: Inicialmente, G es un conjunto de generadores de I, y por tanto $G \subset I$. Los elementos que se le añaden a G son los restos $T = \overline{\mathrm{S}(p,q)}^{G'}$, con p, q elementos de G. Si G está contenido en I, también lo estarán p, q y $\mathrm{S}(p,q)$, y como estamos dividiendo por $G' \subset I$, obtenemos que $G \cup \{T\} \subset I$.
El algoritmo termina cuando G es igual a G'. Esto significa que $\overline{S(p,q)}^{G} = 0$ para todo $p, q \in G$. Por el Teorema 1.49, que G verifique esta condición es equivalente a que sea una base de Groebner G.

Falta por probar que el algoritmo efectivamente concluye. En cada iteración, el conjunto G está constituído por G' (el anterior G) y por los restos no nulos de las sizigias de elementos de G'. Entonces, como $G' \subset G$, se tiene que:

$$\langle \mathrm{LT}(G') \rangle \subset \langle \mathrm{LT}(G) \rangle. \tag{1.13}$$

Además, si $G' \neq G$, tampoco se tiene la igualdad entre $\mathrm{LT}(G')$ y $\mathrm{LT}(G)$. Para probar esto, supongamos que un resto no nulo r de una sizigia se añade al conjunto G'. Por ser el resto de una división por $G', \mathrm{LT}(r)$ no es divisible por ningún término principal de ningún elemento de G', y entonces, $\mathrm{LT}(r) \notin \mathrm{LT}(G')$. Pero $\mathrm{LT}(r) \in \mathrm{LT}(G)$ porque $r \in G$.
La ecuación (1.13)nos dice que los ideales $\langle \mathrm{LT}(G') \rangle$ de las sucesivas iteraciones forman una cadena ascendente de ideales en $K[\boldsymbol{x}]$. Usando la condición de cadena ascendente, se tiene que dicha cadena de ideales debe estabilizarse en un número finito de iteraciones, de forma que $\langle \mathrm{LT}(G') \rangle = \langle \mathrm{LT}(G) \rangle$. Por el razonamiento que acabamos de hacer, esto implica que $G = G'$ y así, el algoritmo termina en un número finito de iteraciones. □

Vamos a ilustrar el algoritmo de Buchberger con un ejemplo:

Ejemplo 1.52. Sea $I = \langle f_1, f_2 \rangle = \langle x^3 - 2xy^2, x^2y - 2y^2 \rangle$ un ideal en $K[x,y]$ y consideremos el orden lexicográfico, con $x > y$.
$\{f_1, f_2\}$ no es una base de Groebner ya que:

$$\mathrm{S}(f_1,f_2) = \frac{x^3y}{x^3}(x^3 - 2xy^2) - \frac{x^3y}{x^2y}(x^2y - 2y^2) = x^3y - 2xy^3 - (x^3y - 2xy^2) = -2xy^3 + 2xy^2.$$

$\mathrm{LT}(S(f_1,f_2)) = -2xy^3 + 2xy^2 \notin \langle \mathrm{LT}(f_1), \mathrm{LT}(f_2) \rangle$.
Nuestro algoritmo consiste en extender el conjunto inicial de generadores con nuevos polinomios de I para obtener una base de Groebner. Si intentamos dividir $\mathrm{S}(f_1,f_2)$ por $F = \{f_1, f_2\}$, obtenemos:

$\mathrm{S}(f_1, f_2) = 0 \cdot f_1 + 0 \cdot f_2 + (-2xy^3 + 2xy^2)$.

Esto nos indica que deberíamos incluír $-2xy^3 + 2xy^2$ en nuestro conjunto de generadores del ideal: $f_3 = -2xy^3 + 2xy^2, F = \{f_1, f_2, f_3\}$.

$\mathrm{S}(f_1, f_2) = f_3 \Rightarrow \overline{\mathrm{S}(f_1, f_2)}^F = 0$.

$\mathrm{S}(f_1, f_3) = \frac{x^3y^3}{x^3} \cdot (x^3 - 2xy) - \frac{x^3y^3}{-2xy^3} \cdot (-2xy^3 + 2xy^2) = 2x^3y^2 - 2xy^4$.

Tras realizar el algoritmo de la división, obtenemos que $\overline{\mathrm{S}(f_1, f_3)}^F = 2xy^2 \neq 0$.

Igual que antes, añadimos $2xy^2$ al conjunto de generadores: $f_4 = 2xy^2, F = \{f_1, f_2, f_3, f_4\}$.

$\overline{\mathrm{S}(f_1, f_2)}^F = \overline{\mathrm{S}(f_1, f_3)}^F = 0$.

$\mathrm{S}(f_1, f_4) = \frac{x^3y^2}{x^3}(x^3 - 2xy) - \frac{x^3y^2}{2xy^2}(2xy^2) = -2xy^3 = 1 \cdot f_3 - 1 \cdot f_4$.

$\overline{\mathrm{S}(f_1, f_4)}^F = 0$.

$\mathrm{S}(f_2, f_3) = \frac{x^2y^3}{x^2y}(x^2y - 2y^2) - \frac{x^2y^3}{-2xy^3}(-2xy^3 + 2xy^2) = x^2y^2 - 2y^4 = y \cdot f_2 - 2y^4 + 2y^3$.

$\overline{\mathrm{S}(f_2, f_3)}^F = -2y^4 + 2y^3$.

Denotamos el polinomio por: $f_5 = -2y^4 + 2y^3$, y ampliamos el conjunto de generadores nuevamente: $F = \{f_1, f_2, f_3, f_4, f_5\}$.

$\overline{\mathrm{S}(f_1, f_2)}^F = \overline{\mathrm{S}(f_1, f_3)}^F = \overline{\mathrm{S}(f_1, f_4)}^F = 0$.

$\mathrm{S}(f_2, f_4) = \frac{x^3y^2}{x^2y}(x^2y - 2y^2) - \frac{x^3y^2}{2x^3y^2}(2x^3y^2 - 2xy^4) = xy^4 - 2xy^3 = \frac{-y}{2} \cdot f_3 - xy^3$.

$\overline{\mathrm{S}(f_2, f_4)}^F = -xy^3$.

Añadimos este polinomio al conjunto de generadores: $f_6 = -xy^3, F = \{f_1, f_2, f_3, f_4, f_5, f_6\}$.

Ahora, los únicos restos que no dan cero son los siguientes:

$\mathrm{S}(f_3, f_6) = \frac{xy^3}{-2xy^3}(-2xy^3 + 2xy^2) - \frac{xy^3}{xy^3}(xy^3) = -2xy^2$.

$\overline{\mathrm{S}(f_3, f_6)}^F = -2xy^2 \neq 0$.

$\mathrm{S}(f_4, f_6) = \frac{x^3y^3}{2x^3y^2}(2x^3y^2 - 2xy^4) - \frac{x^3y^3}{xy^3}(xy^3) = -2y^4 = f_5 - 2y^3$.

$\overline{\mathrm{S}(f_4, f_6)}^F = -2y^3 \neq 0$.

Como estos dos polinomios son monomios que no se dividen el único al otro, debemos añadir ambos a nuestro conjunto de generadores. Denotamos $f_7 = -2xy^2, f_8 = -2y^3$, y nuestro nuevo conjunto de generadores: $F = \{f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8\}$. Ahora es sencillo comprobar que $\overline{\mathrm{S}(f_i, f_j)}^F = 0$ para todo $i, j \in \{1, \ldots, 8\}$. En virtud del Teorema 1.49, F es base de Groebner de I.

Una vez que hemos visto como construír una base de Groebner para un ideal I, vamos ahora a buscar, a partir de ella, una base de Groebner mejor, en el sentido de que no contenga elementos redundantes y sea lo más simple posible:

Lema 1.53. *Sea G una base de Groebner para el ideal de polinomios I. Sea $p \in G$ un polinomio tal que $\mathrm{LT}(p) \in \langle \mathrm{LT}(G - \{p\}) \rangle$. Entonces $G - \{p\}$ es también una base de Groebner de I.*

Demostración. Sea $G = \{g_1, \ldots, g_t, p\}$. Sabemos que $\langle \text{LT}(g_1), \ldots, \text{LT}(g_t), \text{LT}(p)\rangle = \langle \text{LT}(I)\rangle$, y que $\text{LT}(p) \in \langle \text{LT}(G - \{p\})\rangle = \langle \text{LT}(g_1), \ldots, \text{LT}(g_t)\rangle$. Esto implica de forma inmediata que:

$$\langle \text{LT}(g_1), \ldots, \text{LT}(g_t)\rangle = \langle \text{LT}(g_1), \ldots, \text{LT}(g_t), \text{LT}(p)\rangle = \langle \text{LT}(I)\rangle.$$

Y por tanto $\{g_1, \ldots, g_t\} = G - \{p\}$ es una base de Groebner de I. □

Definición 1.54. Una base de Groebner minimal para el ideal I es una base de Groebner de I tal que:

- $\text{LC}(p) = 1$ para todo $p \in G$.
- Para todo $p \in G, \text{LT}(p) \notin \langle \text{LT}(G - \{p\})\rangle$.

Proposición 1.55. *Sean G y G' dos bases de Groebner minimales de un ideal I. Entonces:*

$$\text{LT}(G) = \text{LT}(G').$$

Demostración. Sean $G = \{f_1, \ldots, f_s\}$ y $G' = \{g_1, \ldots, g_t\}$. Por definición de base de Groebner, se tiene la siguiente igualdad:

$$\langle \text{LT}(f_1), \ldots, \text{LT}(f_s)\rangle = \langle \text{LT}(I)\rangle = \langle \text{LT}(g_1), \ldots, \text{LT}(g_t)\rangle.$$

Consideremos el primero de los polinomios de G, f_1. La igualdad anterior nos garantiza que $\text{LT}(f_1) \in \langle \text{LT}(g_1), \ldots, \text{LT}(g_t)\rangle$. Por el Lema 1.13 sabemos que entonces existe $j_1 \in \{1, \ldots, t\}$ tal que $\text{LT}(g_{j_1}) | \text{LT}(f_1)$. Por otro lado, $\text{LT}(g_{j_1}) \in \langle \text{LT}(f_1), \ldots, \text{LT}(f_s)\rangle$, entonces existirá un índice $i_1 \in \{1, \ldots, s\}$ tal que $\text{LT}(f_{i_1}) | \text{LT}(g_{j_1})$. Por ser G una base de Groebner minimal necesariamente se tiene la igualdad $\text{LT}(f_1) = \text{LT}(g_{j_1})$ y entonces ya tenemos probado que $\text{LT}(f_1) \in \text{LT}(G')$.

De forma análoga comprobamos que los términos principales $\text{LT}(f_2), \ldots, \text{LT}(f_s)$ también pertenecen a $\text{LT}(G')$. Si ahora intercambiamos los papeles de G y G' y usamos este mismo razonamiento, es inmediato comprobar que los términos principales $\text{LT}(g_1), \ldots, \text{LT}(g_t)$ pertenecen a $\text{LT}(G)$. □

Definición 1.56. Una base de Groebner reducida para un ideal de polinomios I es una base de Groebner G tal que:

- $\text{LC}(p) = 1$ para todo $p \in G$.
- Para todo $p \in G$, ningún monomio de p pertenece a $\langle \text{LT}(G - \{p\})\rangle$.

Proposición 1.57. *Fijado un orden monomial en $K[x_1, \ldots, x_n]$, para cada ideal no nulo $I \subset K[x_1, \ldots, x_n]$ existe una única base de Groebner reducida.*

Demostración. Primero probaremos que existe al menos una base de Groebner reducida. Sea G una base minimal de I. Decimos que un elemento $g \in G$ es reducido para G si ningún monomio de G pertenece a $\langle \text{LT}(G - \{g\})\rangle$. Nuestro objetivo es modificar G hasta que todos sus elementos sean reducidos. Una primera observación es que si g es reducido para G, entonces g también es reducido para cualquier otra base minimal de I que contenga a g y tenga el mismo conjunto de términos principales. Esto es debido a que la definición de reducido solo involucra a los términos principales.

Ahora, dado $g \in G$, sean $g' = \overline{g}^{G-\{g\}}$ y $G' = (G - \{g\}) \cup \{g'\}$. Queremos ver que G' es otra base de Groebner minimal de I. Para esto, observemos que $\text{LT}(g') = \text{LT}(g)$, ya que cuando dividimos g por $G - \{g\}$, $\text{LT}(g)$ se añade al resto de la división debido a que no es divisible por ningún elemento de $\text{LT}(G - \{g\})$. Esto prueba que $\langle \text{LT}(G')\rangle = \langle \text{LT}(G)\rangle$. Dado que G' está contenido en I, queda claro que G' es una base de Groebner, y también que es minimal. Finalmente, notemos también que g' es reducido para G' por construcción.

Ahora, podemos tomar todos los elementos de G y aplicar el proceso anterior para que todos los elementos sean reducidos. La base de Groebner podría cambiar cada vez que repetimos el proceso, pero si un elemento es reducido, lo sigue siendo siempre y cuando no cambiemos los términos principales de los elementos de la base. Así, repitiendo el proceso las veces que sea necesario, obtenemos una base de Groebner reducida.

Nos falta demostrar la unicidad: Supongamos que G y $\tilde{G}$ son bases de Groebner reducidas para I. Entonces, en particular, G y $\tilde{G}$ son bases de Groebner minimales. y eso implica que tienen los mismos términos principales: $\text{LT}(G) = \text{LT}(G')$. Dado $g \in G$, hay un $\tilde{g} \in \tilde{G}$ tal que $\text{LT}(g) = \text{LT}(\tilde{g})$. Si podemos probar que $g = \tilde{g}$, entonces $G = \tilde{G}$ y tendremos probada la unicidad.

Para probar $g = \tilde{g}$, consideremos $g - \tilde{g} \in I$. Como G es una base de Groebner, tenemos que $\overline{g - \tilde{g}}^{G} = 0$. Además, por 1.55 sabemos que $\text{LT}(g) = \text{LT}(\tilde{g})$. Esto significa que al restarlos, los términos principales se cancelan, y los términos restantes no son divisibles por ninguno de los elementos de $\text{LT}(G) = \text{LT}(G')$ puesto que son bases de Groebner reducidas. Esto prueba que $\overline{g - \tilde{g}}^{G} = g - \tilde{g} = 0$, y entonces $g = \tilde{g}$. □

Con este resultado, queda resuelto el problema de decidir si dos ideales del anillo de polinomios $K[\boldsymbol{x}]$ son iguales:

Corolario 1.58. *Dos ideales no nulos de $K[x_1, \ldots, x_n]$ son iguales si, y sólo si, fijado un orden monomial poseen la misma base de Groebner reducida.*

Capítulo 2

Teoría de la Eliminación

En este capítulo estudiaremos un método sistemático para la resolución de sistemas de ecuaciones polinómicas: el método de eliminación de variables.

Resolver sistemas de ecuaciones polinómicas es extremadamente importante ya que nos permitirá hallar explícitamente los puntos que conforman las variedades afines algebraicas. Recordemos que:

$$V(I) = \{(a_1, \ldots, a_n) \in K^n \ / \ f(a_1, \ldots, a_n) = 0 \ \forall \ f \in I\}.$$

Las bases de Groebner resultarán de utilidad para la demostración de los resultados más importantes que permiten llevar a cabo la resolución de los sistemas: El teorema de Eliminación y el teorema de Extensión. La aplicación más inmediata que mostraremos será resolver el *Problema de Implicitación.*

2.1. Teoremas de Eliminación y Extensión.

Antes de introducir notación y resultados, veamos un ejemplo de resolución de un sistema de ecuaciones:

Ejemplo 2.1. Consideremos el siguiente sistema de ecuaciones polinómicas:

$$\left.\begin{array}{c} x^2 + y^2 = 0 \\ y^2 - z^2 = 1 \\ x^2 + y - z^2 = 0 \end{array}\right\}$$

Consideramos el ideal $I = \langle x^2 + y^2, \ y^2 - z^2 - 1, \ x^2 + y - z^2 \rangle$.

Ahora, consideramos una base de Groebner del ideal I respecto al orden lexicográfico:

$$G = \{x^2 + z^2 + 1, \ y - 2z^2 - 1, \ 4z^4 + 3z^2\}.$$

Las ecuaciones obtenidas igualando los elementos de esta base a cero tienen exactamente las mismas soluciones que las iniciales, pues los dos conjuntos de polinomios generan el mismo ideal. Sin embargo, considerando las ecuaciones dadas por la base de Groebner, observamos que la última ecuación solo involucra a z, y es fácil de resolver:

$$4z^4 + 3z^2 = 0 \Rightarrow z \in \{0, \pm\frac{\sqrt{3}}{2}i\}$$

Sustituyendo estos resultados en $y - 2z^2 - 1 = 0$ podemos obtener los valores de y. Finalmente, con los valores de y y de z, sustituímos en $x^2 + z^2 + 1 = 0$ y obtenemos los valores de x.

Así, las soluciones del sistema serían:

$$\left((i,1,0),\ (-i,1,0),\ (\frac{i}{2},\frac{-1}{2},\frac{\sqrt{3}}{2}i),\ (\frac{-i}{2},\frac{-1}{2},\frac{\sqrt{3}}{2}i),\ (\frac{-i}{2},\frac{-1}{2},\frac{-\sqrt{3}}{2}i),\ (\frac{-i}{2},\frac{-1}{2},\frac{-\sqrt{3}}{2}i)\right).$$

Dos factores clave que nos han permitido resolver el sistema de esta forma han sido:

- Encontrar una ecuación en una sola variable: $4z^4 + 3z^2 = 0$
- Extender las soluciones de esa ecuación al resto de ecuaciones, sustituyendo los valores obtenidos.

La idea básica de la teoría de eliminación es que estos dos procesos puedan llevarse a cabo de forma general. Para justificar dichos resultados es necesario definir los ideales de eliminación:

Definición 2.2. Fijemos un entero $k \in \{0, \ldots, n-1\}$. Dado un ideal $I \subset K[x_1, \ldots, x_n]$, el ideal de $K[x_{k+1}, \ldots, x_n]$ definido por

$$I_k := I \cap K[x_{k+1}, \ldots, x_n]$$

se denomina ideal de eliminación k-ésimo de I.

Si $I = \langle f_1, \ldots, f_s \rangle$, el ideal I_k proporciona las ecuaciones que verifican los puntos de $\mathbf{V}(I)$, que no contienen a las variables $x_1, \ldots, x_k$ y que se pueden construir a partir de las ecuaciones $f_1 = \cdots = f_s = 0$ dadas por el ideal original I.

Para aclarar este concepto, consideremos los siguientes ejemplos

Ejemplo 2.3. Sea $I \subset K[x_1, x_2, x_3, x_4, x_5]$ el ideal

$$I = \langle x_1^3 - 2x_2 + x_4,\ 7x_2^2 + x_4 - x_5,\ x_3^2 + 5x_4^4,\ x_5 \rangle.$$

En este caso, podemos decir que los generadores de I son adecuados para eliminar variables, ya que se puede comprobar que:

$$\begin{aligned} I_0 &= I \\ I_1 &= \langle 7x_2^2 + x_4 - x_5,\ x_3^2 + 5x_4^4,\ x_5 \rangle \\ I_2 &= \langle x_3^2 + 5x_4^4,\ x_5 \rangle \\ I_3 &= I_4 = \langle x_5 \rangle \end{aligned}$$

Ejemplo 2.4. Pero no siempre es inmediato hallar los ideales de eliminación de un ideal a partir de un sistema de generadores.

Por ejemplo, sea $I = \langle x_1, x_1 + x_2 + x_3, x_3 \rangle \subset K[x_1, x_2, x_3, x_4]$. En este caso, en dos de los generadores del ideal aparece la variable x_1. Pero esto no significa que el primer ideal de eliminación I_1 sea igual a $\langle x_3 \rangle$. Eligiendo otro sistema de generadores $I = \langle x_1, x_2, x_3 \rangle$ es muy sencillo ver que:

$$I_0 = I, \quad I_1 = \langle x_2, x_3 \rangle, \quad I_2 = \langle x_3 \rangle, \quad I_3 = \{0\}.$$

Observación 2.5. El problema de eliminación consiste en, dado un ideal $I \subset K[x_1, \ldots, x_n]$, encontrar un sistema de generadores del ideal $I_k = I \cap K[x_{k+1}, \ldots, x_n]$, para $0 \leq k < n$. Es decir, se trata de encontrar un sistema de generadores del ideal $I \subset K[x_1, \ldots, x_n]$ que contenga a un sistema de generadores de I_k, para cada $k \in \{0, \ldots, n-1\}$. El siguiente teorema nos muestra cómo resolver este problema utilizando bases de Groebner respecto a un orden monomial adecuado, que nos permita eliminar variables.

Definición 2.6. Sea $\boldsymbol{y} = \{x_1, \ldots, x_k\} \subset \boldsymbol{x} = \{x_1, \ldots, x_k, x_{k+1}, \ldots, x_n\}$ una colección de variables y $\boldsymbol{z} = \boldsymbol{x} \setminus \boldsymbol{y}$. Diremos que un orden monomial en $K[\boldsymbol{x}]$ elimina las variables $\boldsymbol{y}$ si siempre que $\boldsymbol{y}^{\boldsymbol{\alpha}} > \boldsymbol{y}^{\boldsymbol{\beta}}$ se verifica que $\boldsymbol{y}^{\boldsymbol{\alpha}}\boldsymbol{z}^{\boldsymbol{\sigma}} > \boldsymbol{y}^{\boldsymbol{\beta}}\boldsymbol{z}^{\boldsymbol{\nu}}$, para cualesquiera monomios $\boldsymbol{z}^{\boldsymbol{\sigma}}\boldsymbol{y}\boldsymbol{z}^{\boldsymbol{\nu}}$.

Ejemplo 2.7. El orden monomial lexicográfico con $x_1 > x_2 > \cdots > x_n$ elimina las variables $\boldsymbol{y} = \{x_1, \ldots, x_k\}$. El orden graduado lexicográfico no elimina ninguna variable.

Teorema 2.8 (Teorema de Eliminación)**.** *Consideremos en $K[x_1, \ldots, x_n]$ el orden monomial lexicográfico determinado por $x_1 > x_2 > \cdots > x_n$. Para cada $k \in \{0, \ldots, n-1\}$ consideremos en $K[x_{k+1}, \ldots, x_n]$ el orden monomial inducido por el de $K[x_1, \ldots, x_n]$. Sea $I \subset K[x_1, \ldots, x_n]$ un ideal y G una base de Groebner de I. Entonces, en $K[x_{k+1}, \ldots, x_n]$, el conjunto $G_k = G \cap K[x_{k+1}, \ldots, x_n]$ es una base de Groebner del ideal de eliminación k-ésimo $I_k \subset K[x_{k+1}, \ldots, x_n]$.*

Demostración. Fijemos $k \in \{0, \ldots, n-1\}$. Para un subconjunto $B \subset K[x_{k+1}, \ldots, x_n]$ denotaremos por $\langle B \rangle_k$ el ideal de $K[x_{k+1}, \ldots, x_n]$ generado por B. Demostraremos que

$$\langle \mathrm{LT}(G_k) \rangle_k = \langle \mathrm{LT}(I_k) \rangle_k.$$

En efecto, como $G_k \subset I_k$, trivialmente se tiene que $\langle \text{LT}(G_k)\rangle_k \subset \langle \text{LT}(I_k)\rangle_k$; veamos que se verifica el otro contenido $\langle \text{LT}(I_k)\rangle_k \subset \langle \text{LT}(G_k)\rangle_k$. Para cualquier $f \in I_k$, se tiene que $f \in I$. En el anillo $K[x_1, \ldots, x_n]$, G es una base de Groebner para el ideal I, entonces existirá un elemento $g \in G$ tal que $\text{LT}(g) \mid \text{LT}(f)$ (en $K[x_1, \ldots, x_n]$); como $f \in I_k$, $\text{LT}(f) \in K[x_{k+1}, \ldots, x_n]$ y necesariamente $\text{LT}(g) \in K[x_{k+1}, \ldots, x_n]$. Además, como $\text{LT}(g)$ es el término de mayor grado de $g \in K[x_1, \ldots, x_n]$ para el orden lexicográfico determinado por $x_1 > x_2 > \ldots > x_n$, en todos los demás términos de g no aparece ninguna de las variables $x_1, \ldots, x_k$, es decir $g \in G_k$. Por tanto $\text{LT}(f) \in \langle \text{LT}(G_k)\rangle_k$. □

Este teorema nos permite simplificar los sistemas de ecuaciones polinómicas para reducirlos a sistemas equivalentes de modo que las ecuaciones involucren de modo escalonado las variables del sistema original, y que por tanto puedan ser resueltos comenzando con las posibles soluciones parciales de las ecuaciones con pocas variables imponiendo después el resto de ecuaciones y comprobando qué soluciones parciales se pueden extender a una solución de todo el sistema.

Ahora nos centraremos en discutir que ocurre con el paso de extensión de soluciones del sistema: ¿Se puede llevar a cabo siempre? ¿Todas las soluciones del sistema 'reducido' pueden ser extendidas a soluciones del sistema original? Antes de comenzar a exponer resultados encaminados a responder estas preguntas, necesitamos introducir una serie de conceptos que tendrán una gran relevancia a lo largo de todo el capítulo:

Definición 2.9. Sea K^n el espacio afín de dimensión n. Se define la proyección k-ésima como la aplicación que lleva cada punto del espacio afín en sus $n-k$ últimas componentes:

$$\begin{array}{rcl} \pi_k : K^n & \longrightarrow & K^{n-k} \\ (a_1, \ldots, a_n) & \mapsto & (a_{k+1}, \ldots, a_n). \end{array}$$

El *Teorema de extensión* estudia cuales de las soluciones de las ecuaciones obtenidas eliminando las k primeras variables pueden ser extendidas a soluciones del sistema completo, es decir, que puntos del espacio afín K^{n-k} forman parte de la imagen de las soluciones del sistema completo a través de la aplicación π_k. En términos de variedades algebraicas:

> El *Teorema de extensión* estudia la relación entre $\pi_k(\mathbf{V}(I))$, la proyección en K^{n-k} de una variedad afín $\mathbf{V}(I) \subset K^n$, y la variedad $\mathbf{V}(I_k) \subset K^{n-k}$ definida por el k-ésimo ideal de eliminación.

Notación 2.10. Dado un orden monomial, una presentación estándar de un polinomio $f \in K[\boldsymbol{x}]$ respecto a un subconjunto finito $G \subset K[\boldsymbol{x}]$ es cualquier expresión de la forma:

$$f = \sum_{g \in G} h_g \cdot g, \qquad (\text{con } h_g \in K[\boldsymbol{x}])$$

tal que, siempre que $h_g \neq 0$, se verifique $\text{MGRAD}(h_g g) \leqslant \text{MGRAD}(f)$, o equivalentemente en términos de monomios, $\text{LM}(h_g) \cdot \text{LM}(g) \leqslant \text{LM}(f)$.

Usando esta terminología una base de Groebner de un ideal $I \subset K[\boldsymbol{x}]$ es un subconjunto finito de polinomios $G = \{g_1, \ldots, g_t\} \subset I \subset K[\boldsymbol{x}]$ con la propiedad de que cada elemento $f \in I$ admite una presentación estándar con respecto a G.

Notación 2.11. Fijado $b = (b_{k+1}, \ldots, b_n) \in K^{n-k}$ denotamos por σ_b el homomorfismo evaluación en b:

$$\begin{array}{rccc} \sigma_b : & K[x_1, \ldots, x_n] & \longrightarrow & K[x_1, \ldots, x_k] \\ & f & \mapsto & f(x_1, \ldots, x_k, b_{k+1}, \ldots, b_n). \end{array}$$

Es importante darse cuenta de que:

$$b \in \pi_k(\mathbf{V}(I)) \iff \mathbf{V}(\sigma_b(I)) \neq \varnothing.$$

Además, como $\sigma_b(f) = f(b)$ para $f \in K[x_{k+1}, \ldots, x_n]$, tenemos que $\pi_k(\mathbf{V}(I)) \subset \mathbf{V}(I_k)$.

Ahora procederemos a probar el *teorema de extensión*, que nos da una condición suficiente para garantizar que dado un sistema de ecuaciones polinómicas en n variables correspondientes a un ideal $I \subset K[x_1, \ldots, x_n]$, y una solución parcial $(a_2, \ldots, a_n)$ de las ecuaciones correspondientes al primer ideal de eliminación de I, podamos extender esta solución para obtener una solución del sistema original.

Notación 2.12. Un polinomio $f \in K[x_1, \ldots, x_n]$ se puede considerar como un polinomio en la variable x_1 con coeficientes en el anillo $K[x_2, \ldots, x_n] = R$. Denotaremos con $\deg_{x_1}(f)$ el grado de f como polinomio del anillo $R[x]$ Si consideramos el orden lexicográfico con $x_1 > x_2 > \ldots > x_n$, dado un polinomio $f \in K[x_1, \ldots, x_n]$, con $\text{LT}(f) = c \cdot \boldsymbol{x}^{\boldsymbol{\alpha}}$, entonces $\deg_{x_i}(f) = \alpha_i$

Proposición 2.13. *Sea $G = \{g_1, \ldots, g_s\}$ una base de Groebner para un ideal I del anillo de polinomios en n variables $K[\boldsymbol{x}]$ respecto al orden lexicográfico, con $x_1 > x_2 > \ldots > x_n$. Dado $(a_2, \ldots, a_n) \in K^{n-1}$, sea $\sigma : K[x_1, \ldots, x_n] \longrightarrow K[x_1]$ el K-homomorfismo de anillos definido por:*

$$\sigma(x_1) = x_1 \qquad \sigma(x_i) = a_i \text{ para todo } i \geqslant 2.$$

Supongamos que G contiene un polinomio cuyo coeficiente principal no es aniquilado por σ. Entonces $\sigma(I) = \langle \sigma(g) \rangle$, donde $g \in G$ es de (multi)-grado mínimo con la propiedad de que $\sigma(\text{LC}(g)) \neq 0$.

Demostración. Dado un polinomio $0 \neq l \in K[x_1]$ denotaremos su grado por $\deg(l)$. Escojamos $g \in G$ de grado mínimo con la propiedad de que $\sigma(\text{LC}(g)) \neq 0$, y fijemos

$\mathbf{D} = (D_1, \ldots, D_n) = \text{MGRAD}(g)$. Primero vamos a probar que para todo $\delta \in \mathbb{N}$ se cumple que:

$$\text{Dado } h \in G: \ \text{MGRAD}(h) < \mathbf{D} \Rightarrow \ \deg(\sigma(h)) \leqslant \ \deg_{x_1}(h) - \delta.$$

Esto significa que, si $\text{MGRAD}(h) < \mathbf{D}$ entonces h es aniquilado por σ. Lo demostraremos por inducción en δ:

El caso $\delta = 1$ es inmediato, ya que la elección de g nos asegura que el coeficiente principal de h es aniquilado por σ. Ahora probaremos el caso general usando nuestra hipótesis de inducción. Sea $h \in G$ con $\mathbf{d} = \text{MGRAD}(h) < \mathbf{D}$. Consideremos el polinomio:

$$\mathrm{S}_1 = \text{LC}(g) \cdot \boldsymbol{x}^{\mathbf{D}-\mathbf{d}} \cdot h - \text{LC}(h) \cdot g.$$

Notemos que S_1 es una sizigia. Por construcción, se produce una cancelación en el monomio de grado más alto, y por tanto, $\text{MGRAD}(S_1) < \mathbf{D}$.

Sea $\mathrm{S}_1 = \sum_{j \in G} f_j \cdot j$ una presentación estándar. Si $j \in G$ es tal que $f_j \neq 0$, entonces se tiene la desigualdad: $\text{MGRAD}(f_j) + \text{MGRAD}(j) \leqslant \text{MGRAD}(\mathrm{S}_1) < \mathbf{D}$. En particular $\text{MGRAD}(j) < \mathbf{D}$, y entonces podemos aplicarle a j nuestra hipótesis de inducción: $\deg(\sigma(j)) \leqslant \ \deg_{x_1}(j) - \delta$. De esta forma, siendo $f_j \neq 0$,

$$\deg(\sigma(f_j \cdot j)) = \ \deg(\sigma(f_j)) + \ \deg(\sigma(j)) \leqslant \ \deg_{x_1}(f_j) + \ \deg_{x_1}(j) - \delta < D_1 - \delta.$$

Y por tanto, finalmente:

$$\begin{aligned} D_1 - \delta > \ \deg(\sigma(S_1)) &= \ \deg(\sigma(\text{LC}(g) \cdot \boldsymbol{x}^{\mathbf{D}-\mathbf{d}} \cdot h - \text{LC}(h) \cdot g))) = \\ &= \ \deg(\sigma(\text{LC}(g)) \cdot x_1^{D_1 - d_1} \cdot \sigma(h)) = \ \deg(\sigma(h)) + D_1 - d_1. \end{aligned}$$

De aquí se concluye que $\deg(\sigma(h)) < d_1 - \delta = \ \deg_{x_1}(h) - \delta$.

Ahora probaremos que $\sigma(h) \in \langle \sigma(g) \rangle$ para todo $h \in G$ por inducción en $\deg_{x_1}(h)$: Asumamos, por nuestra hipótesis de inducción, que hemos probado que $\sigma(j) \in \langle \sigma(g) \rangle$ para todo $j \in G$ con $\text{MGRAD}(j) < \text{MGRAD}(h) = \mathbf{d} \geqslant \mathbf{D}$. Podemos hacer esto porque si $\text{MGRAD}(j) < \text{MGRAD}(h) < \mathbf{D}$ entonces $\sigma(j) = 0 \in \langle \sigma(g) \rangle$. Consideremos ahora el polinomio:

$$\mathrm{S}_2 = \text{LC}(g) \cdot h - \text{LC}(h) \cdot \boldsymbol{x}^{\mathbf{d}-\mathbf{D}} \cdot g \in I.$$

Observemos que, por construcción, $\text{MGRAD}(\mathrm{S}_2) < \mathbf{d}$. Si tomamos una presentación estándar de dicho polinomio, $\mathrm{S}_2 = \sum_{j \in G} f_j \cdot j$, tenemos la siguiente desigualdad: Para $j \in G$, con $f_j \neq 0, \text{MGRAD}(f_j) + \text{MGRAD}(j) < \mathbf{d}$. En particular, $\text{MGRAD}(j) < \mathbf{d}$, por lo que $\sigma(j) \in \langle \sigma(g) \rangle$.

Como $\text{LC}(g) \cdot h = S_2 + \text{LC}(h) \cdot \boldsymbol{x}^{\mathbf{d}-\mathbf{D}} \cdot g = \sum_{j \in G} f_j \cdot j + \text{LC}(h) \cdot \boldsymbol{x}^{\mathbf{d}-\mathbf{D}} \cdot g$, y $\sigma(\text{LC}(g)) \neq 0$, usando el homomorfismo se concluye que:

$$\sigma(h) \in \langle \sigma(j) \mid f_j \neq 0 \rangle + \langle \sigma(g) \rangle \subset \langle \sigma(g) \rangle \text{ por la hipótesis de inducción.} \qquad \square$$

Teorema 2.14 (Teorema de Extensión)**.** *Sea $I \subset K[x_1, \ldots, x_n]$ un ideal, con K algebraicamente cerrado, y sea $(a_2, \ldots, a_n) \in \boldsymbol{V}(I_1)$ un cero del primer ideal de eliminación. Supongamos que existe un polinomio $0 \neq f \in I$ tal que*

$$f = \sum_{i=0}^{t} c_i \cdot x_1^i$$

siendo $c_i \in K[x_2, \ldots, x_n]$ y $deg_{x_1}(f) = t$, tal que $c_t(a_2, \ldots, a_n) \neq 0$. Entonces existe un $a_1 \in K$ tal que $(a_1, a_2, \ldots, a_n) \in \boldsymbol{V}(I)$.

Demostración. Consideramos el K-homomorfismo

$$\begin{array}{rccc} \sigma_{(a_2,\ldots,a_n)}: & K[x_1, \ldots, x_n] & \longrightarrow & K[x_1] \\ & f(x_1, \ldots, x_n) & \mapsto & f(x_1, a_2, \ldots, a_n). \end{array}$$

Sea G una base de Groebner de $I \subset K[\boldsymbol{x}]$ con respecto al orden lexicográfico dado por $x_1 > x_2 > \ldots > x_n$. Es importante elegir este orden para que la variable x_1 sea mayor que todas las demás.

Con esta elección, dado un polinomio $f \in I$, en una presentación estándar de dicho polinomio; $f = \sum_{g \in G} h_g \cdot g$, se tiene que: $\deg_{x_1}(h_g \cdot g) = \deg_{x_1}(f)$ para todo g con $h_g \neq 0$. Por ser G una base de Groebner de I, $\text{LC}(f) \in \langle \text{LC}(G) \rangle$ y entonces, $\langle \text{LC}(G) \rangle \nsubseteq \ker(\sigma)$.

Con esto, se cumplen todas las hipótesis de la Proposición 2.13, y por tanto concluímos que existe $g \in G$ de forma que $0 \neq \sigma(I) = \langle \sigma(g) \rangle \subset K[x_1]$. De esta forma, si $a_1 \in K$ es un cero de $\sigma(g)$, entonces $(a_1, a_2, \ldots, a_n) \in \mathbf{V}(I)$. □

A continuación, expondremos diferentes ejemplos de situaciones que pueden ocurrir al realizar el paso de extensión:

Ejemplo 2.15. Un ejemplo trivial consiste en considerar un sistema $f_1 = \ldots = f_s = 0$ en el anillo de polinomios $K[x_1, \ldots, x_n]$, con $f_1, \ldots, f_s \in K[x_2, \ldots, x_n]$.

En este caso, sea cual sea el sistema, la variable x_1 no aparece en ninguna de las ecuaciones. Supongamos que $(a_2, \ldots, a_n)$ es una solución parcial del sistema. Entonces el punto $(a, a_2, \ldots, a_n)$, con $a \in K$, es siempre una solución del sistema original.

Ejemplo 2.16. Consideramos la variedad afín $V \subset \mathbb{C}^3$ determinada por las ecuaciones:

$$xy = 1, \qquad xz = 1.$$

Para resolver el sistema utilizando el proceso de eliminación y extensión, consideramos el ideal $I = \langle xy - 1, xz - 1 \rangle$. A continuación construímos una base de Groebner de dicho ideal respecto del orden lexicográfico, con $x > y > z$: $G = \{xy - 1, xz - 1, y - z\}$, y por el Teorema 2.8 sabemos que $G_1 = \{y - z\}$ es una base de Groebner del ideal I_1.

Entonces las soluciones parciales del sistema obtenido eliminando la primera variable, $\mathbf{V}_{\mathbb{C}^2}(I_1)$, son los puntos de la recta $y = z$. Por otro lado, la imagen de V mediante la proyección

$$\begin{array}{rccc} \pi_1 : & \mathbb{C}^3 & \longrightarrow & \mathbb{C}^2 \\ & (x, y, z) & \mapsto & (y, z) \end{array}$$

es el conjunto $\pi_1(V) = \{(a, a) \in \mathbb{C}^2 : a \neq 0\}$.

Todas las soluciones parciales del sistema pueden ser extendidas a soluciones del sistema original exceptuando la solución $(0, 0)$. Esto ocurre debido a que si consideramos las ecuaciones del sistema original, $xy = 1;\ xz = 1$, e imponemos $y = 0$ y $z = 0$, el sistema resultante es $0 = 1$, que no posee solución para ningún valor de la variable x. En cambio si tomamos como solución parcial el punto (a, a), con $a \neq 0$, el punto $(1/a, a, a)$ es solución del sistema original.

2.2. Teorema de Clausura.

Nuestro objetivo en esta sección es dar una interpretación geométrica a los resultados que acabamos de demostrar. Sea $I \subset K[x_1, \ldots, x_n]$ un ideal. Con la notación establecida en la sección anterior, $\pi_k(\mathbf{V}(I)) \subset \mathbf{V}(I_k)$. Si nos fijamos detenidamente en qué significan geométricamente estos conjuntos, la inclusión es obvia: $\mathbf{V}(I_k) \subset K^{n-k}$ es el conjunto de todas las soluciones del sistema obtenido al eliminar las k primeras variables, y $\pi_k(\mathbf{V}(I))$ es el conjunto de ceros $(a_{k+1}, \ldots, a_n) \in K^{n-k}$ del ideal I_k que pueden extenderse a soluciones en K^n del sistema original. Es decir, denotando $V = \mathbf{V}(I)$:

$$\pi_k(V) = \{(a_{k+1}, \ldots, a_n) \in \mathbf{V}(I_k) : \exists\ (a_1, \ldots, a_k) \in K^k, (a_1, \ldots, a_k, a_{k+1}, \ldots, a_n) \in V\}.$$

Desde el punto de vista geométrico, las soluciones de un sistema de ecuaciones polinómicas en n variables pertenecen al espacio afín K^n. Lo que nos dice el teorema de eliminación es que, respecto al orden lexicogrñafico con $x_1 > \ldots > x_n$, teniendo una base de Groebner G de nuestro ideal $I \subset K[x_1, \ldots, x_n]$ podemos hallar una base de Groebner de su ideal de eliminación k-ésimo considerando los elementos de G que no involucran a las variables eliminadas. Por un lado, podemos proyectar las soluciones del sistema original en las $n - k$ últimas variables. Por otro lado podemos calcular en K^{n-k} los ceros de las ecuaciones $G \cap K[x_{k+1}, \ldots, x_n]$.

Uno de los problemas que encontramos en las proyecciones $\pi_k : K^n \longrightarrow K^{n-k}$ es que la proyección no es un morfismo cerrado para la topología de Zariski, es decir, aunque nuestro conjunto $V \subset K^n$ sean las soluciones de una familia de ecuaciones polinómicas $I \subset K[x_1, \ldots, x_n]$, al proyectarlo esta propiedad no tiene por que conservarse. Lo que nos interesa averiguar es que relación hay entre ambos conjuntos.

Si nos fijamos detenidamente en las definiciones que hemos dado previamente, es fácil darse cuenta de que el conjunto de soluciones del sistema después de proyectarlo es precisamente el conjunto $\mathbf{V}(I_k)$, mientras que el conjunto de soluciones del sistema original proyectado en el espacio afín K^{n-k} es $\pi_k(\mathbf{V}(I))$.

Visto de este modo, ya tenemos una primera relación entre ambos conjuntos de soluciones, pues sabemos que $\pi_k(\mathbf{V}(I)) \subset \mathbf{V}(I_k)$. El siguiente teorema, denominado Teorema de Clausura, establece otra relación muy interesante entre ambos conjuntos: $\mathbf{V}(I_k)$ es la clausura de Zariski de $\pi_k(\mathbf{V}(I))$.

Teorema 2.17 (Teorema de Clausura)**.** *Sea K un cuerpo algebraicamente cerrado, $V = \boldsymbol{V}(f_1, \ldots, f_s) \subset K^n$, y sea I_k el ideal de eliminación k-ésimo de $I = \langle f_1, \ldots, f_s \rangle$ para un entero $0 \leqslant k < n$. Entonces $\boldsymbol{V}(I_k)$ es la variedad más pequeña que contiene a $\pi_k(\boldsymbol{V}(I)) \subset K^{n-k}$.*

Demostración. Por simplicidad escribiremos $\pi_k(V)$ en lugar de $\pi_k(\mathbf{V}_K(I))$. Para ver que $\mathbf{V}(I_k)$ es la menor variedad que contiene a $\pi_k(V)$, en virtud de la Proposición 1.5, es equivalente demostrar que $\mathbf{V}(I_k) = \mathbf{V}(\mathbf{I}(\pi_k(V)))$. Como sabemos que $\pi_k(V) \subset \mathbf{V}(I_k)$ y $\mathbf{V}(\mathbf{I}(\pi_k(V)))$ es la variedad más pequeña que contiene a $\pi_k(V)$, la inclusión $\mathbf{V}(\mathbf{I}(\pi_k(V))) \subset \mathbf{V}(I_k)$ es inmediata.

Para ver la otra inclusión, sea $f \in \mathbf{I}(\pi_k(V)) \subset K[x_{k+1}, \ldots, x_n]$, es decir, $f(a_{k+1}, \ldots, a_n) = 0$ para todo $(a_{k+1}, \ldots, a_n) \in \pi_k(V)$. Si consideramos f como un polinomio en $K[x_1, \ldots, x_n]$, es claro que $f(a_1, \ldots, a_n) = 0$ para todo $(a_1, \ldots, a_n) \in V$ ya que f no involucra a las variables $x_1, x_2, \ldots, x_k$. Por el Teorema 1.9 (Teorema de los ceros de Hilbert), existe un entero m tal que $f^m \in \langle f_1, \ldots, f_s \rangle$, y de nuevo, f^m no involucra a las variables $x_1, x_2, \ldots, x_k$, por tanto, $f^m \in I \cap K[x_{k+1}, \ldots, x_n] = I_k$ y entonces $f \in \sqrt{I_k}$, lo cual implica que $\mathbf{I}(\pi_k(V)) \subset \sqrt{I_k}$. Entonces, como la aplicación $\mathbf{V}$ invierte las inclusiones, se tiene que

$$\mathbf{V}(I_k) = \mathbf{V}(\sqrt{I_k}) \subset \mathbf{V}(\mathbf{I}(\pi_k(V))). \qquad \square$$

El siguiente resultado se verifica para cualquier $k \in \{1, 2, \ldots, n\}$, pero su demostración requieren técnicas más sofisticadas que no hemos tratado en este trabajo.

Teorema 2.18 (Teorema de Clausura para $k = 1$)**.** *Bajo las hipótesis del teorema anterior:*

1. *El conjunto $\mathbf{V}(I_1) \subset K^{n-1}$ es la variedad afín más pequeña que contiene a $\pi_1(V)$.*
2. *Si $V \neq \varnothing$ entonces existe una variedad $X \subsetneq \mathbf{V}(I_1) \subset K^{n-1}$ tal que $X \cup \pi_1(V) = \mathbf{V}(I_1)$.*

Demostración. El primer enunciado es un caso particular del teorema anterior. Veamos la demostración del segundo.

Consideremos cada uno de los generadores $f \in \{f_1, \ldots, f_s\}$ no nulos del ideal I escrito como un polinomio en la variable x_1 con coeficientes en $K[x_2, \ldots, x_n]$:

$$f = c_f x_1^{d_f} + \text{ términos de menor grado en } x_1, \qquad c_f \in K[x_2, \ldots, x_n],$$

siendo $\deg_{x_1} f = d_f$. Para $f = 0$, denotaremos $c_f = 0$.

Se verifica que

$$(\mathbf{V}(c_{f_1}, \ldots, c_{f_s}) \cap \mathbf{V}(I_1)) \cup \pi_1(V) = \mathbf{V}(I_1).$$

En efecto, el contenido $(\mathbf{V}(c_{f_1}, \ldots, c_{f_s}) \cap \mathbf{V}(I_1)) \cup \pi_1(V) \subset \mathbf{V}(I_1)$ es trivial, veamos que se verifica el otro contenido. Dado $(a_2, \ldots, a_n) \in \mathbf{V}(I_1)$, si $(a_2, \ldots, a_n) \notin \mathbf{V}(c_{f_1}, \ldots, c_{f_s})$ entonces, por el Teorema de Extensión, existirá un punto de la forma $(a_1, a_2, \ldots, a_n) \in V$, es decir se tendría que $(a_2, \ldots, a_n) = \pi_1(a_1, a_2, \ldots, a_n) \in \pi_1(V)$.

Sea $X \subset K^{n-1}$, el subconjunto algebraico $X := \mathbf{V}(c_{f_1}, \ldots, c_{f_s}) \cap \mathbf{V}(I_1)$. Si $X \subsetneq \mathbf{V}(I_1)$ habríamos demostrado el resultado enunciado. Supongamos que $X = \mathbf{V}(I_1)$, es decir que $\mathbf{V}(I_1) \subset \mathbf{V}(c_{f_1}, \ldots, c_{f_s})$ o equivalentemente, por el teorema de los ceros, que $c_{f_1}, \ldots, c_{f_s} \in \sqrt{I_1} \subset K[x_2, \ldots, x_n]$. En particular $c_{f_1}, \ldots, c_{f_s} \in \sqrt{I} \subset K[x_1, x_2, \ldots, x_n]$ y

por tanto $V = \mathbf{V}(f_1, \ldots, f_s, c_{f_1}, \ldots, c_{f_s})$. Sustituyendo I por el ideal

$$I' = \langle f_1, \ldots, f_s, c_{f_1}, \ldots, c_{f_s} \rangle$$

es sencillo comprobar que $V = \mathbf{V}(\widetilde{I})$ siendo

$$\widetilde{I} := \langle f_1 - c_{f_1}^{d_{f_1}}, \ldots, f_s - c_{f_s}^{d_{f_1}}, c_{f_1}, \ldots, c_{f_s} \rangle.$$

Cada nuevo generador del ideal $\widetilde{I}$ de la forma $\widetilde{f_i} := f_i - c_{f_i}^{d_{f_i}}$ que no es cero tiene grado en x_1 estrictamente menor que el grado de f_i. Sustituyendo el ideal I por el ideal $\widetilde{I}$ para determinar V, $V = \mathbf{V}(\widetilde{I})$, y repitiendo el algoritmo inicial para el ideal $\widetilde{I}$ definimos un conjunto algebraico $\widetilde{X} \subset \mathbf{V}(I_1) \subset K^{n-1}$ tal que $\mathbf{V}(I_1) = \mathbf{V}(\widetilde{I_1}) = \widetilde{X} \cup \pi_1(V)$.

Si en esta iteración el conjunto $\widetilde{X}$ sigue siendo igual a $\mathbf{V}(\widetilde{I_1})$, repetimos el proceso hasta que el conjunto obtenido $\widetilde{X}$ sea un subconjunto propio de $\mathbf{V}(\widetilde{I_1}) = \mathbf{V}(I_1)$, y entonces habríamos demostrado el enunciado. En cada iteración los grados en x_1 de los generadores del ideal $\widetilde{I_1}$ es cero o estrictamente menor que el de los generadores del ideal anterior I'. Si al iterar el proceso los generadores son de grado 0 en x_1, entonces cualquier $(a_2, \ldots, a_n) \in \mathbf{V}(I_1) \subset K^{n-1}$ es una solución parcial del sistema original, ya que que $(a, a_2, \ldots, a_n) \in V$, para cualquier $a \in K$; es decir, $X = \varnothing$ y $\pi_1(V) = \mathbf{V}(I_1)$.

□

2.3. Problema de implicitación.

Una variedad afín algebraica $V \subset K^n$ no siempre viene determinada mediante ecuaciones polinómicas igualadas a cero. En ocasiones, se describen las coordenadas de los puntos de una variedad afín recurriendo al uso de expresiones algebraicas en función de ciertos parámetros. El *problema de implicitación* consiste en transformar las expresiones paramétricas en ecuaciones implícitas que determinen todos los puntos dados por la parametrización.

Observación 2.19. Uno de los problemas inmediatos que se presentan es que el conjunto de puntos dados por una parametrización puede no ser igual a una variedad afín.

Ejemplo 2.20. Una de las parametrizaciones de la circunferencia de radio unidad es la siguiente:

$$x = \frac{1-t^2}{1+t^2}, \qquad y = \frac{2t}{1+t^2}, \qquad t \in K.$$

Notemos que, sin embargo, x no toma el valor -1, sea cual sea el valor de t:

$$x = -1 = \frac{1-t^2}{1+t^2} \Rightarrow 1 - t^2 = -1 - t^2 \Rightarrow 1 = -1.$$

Es decir, el punto $(-1, 0)$ pertenece a la circunferencia pero es un punto que no viene dado por la parametrización.

Surgen de forma natural dos preguntas: ¿Cuándo una parametrización nos proporciona todos los puntos de una variedad? Y en el caso de que no sea así, ¿Cómo encontramos los puntos de una variedad que no vienen dados por la parametrización?

2.3.1. Parametrización polinómica.

Resolveremos primero el caso de que la parametrización sea polinómica. Consideremos una parametrización de un subconjunto de K^n dado por una expresión de la forma

$$\begin{cases} x_1 &= f_1(t_1, \ldots, t_m) \\ x_2 &= f_2(t_1, \ldots, t_m) \\ \vdots & \qquad \vdots \\ x_n &= f_n(t_1, \ldots, t_m) \end{cases}$$

donde $f_1, \ldots, f_n \in K[t_1, \ldots, t_m]$ son polinomios en las variables $t_1, \ldots, t_m$. Podemos visualizar esta parametrización como la aplicación

$$F : K^m \longrightarrow K^n$$

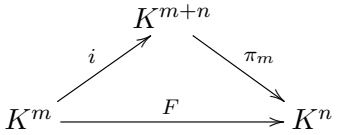
definida por: $F(t_1,\ldots,t_m) = (f_1(t_1,\ldots,t_m),\ldots,f_n(t_1,\ldots,f_m))$.
De esta forma, el conjunto parametrizado viene dado por $F(K^m) \subset K^n$. Por tanto, nuestro problema consiste en hallar la menor variedad afín de K^n que contiene a $F(K^m)$, y para ello vamos a recurrir al proceso de eliminación visto en las secciones anteriores.

Consideramos el conjunto algebraico $V = \mathbf{V}(x_1 - f_1,\ldots,x_n - f_n) \subset K^{m+n}$, cuyos puntos son de la forma $(t_1,\ldots,t_m,f_1(t_1,\ldots,t_m),\ldots,f_n(t_1,\ldots,t_m))$. El conjunto V es el grafo de la función F, es decir, la imagen de la aplicación

$$i : K^m \longrightarrow K^{m+n}$$

definida por: $i(t_1,\ldots,t_m) = (t_1,\ldots,t_m,f_1(t_1,\ldots,t_m),\ldots,f_n(t_1,\ldots,t_m))$.

Consideremos el siguiente diagrama conmutativo:



A la vista del diagrama, la aplicación F puede descomponerse en $F = \pi_m \circ i$. Además, $i(K^m) = V$, y se sigue la igualdad

$$F(K^m) = \pi_m(i(K^m)) = \pi_m(V), \tag{2.1}$$

que nos dice que la imagen de la parametrización es la proyección de su grafo en sus n últimas componentes. Ahora, podemos usar resultados vistos en la teoría de la eliminación para hallar la variedad afín más pequeña que contiene a $F(K^m)$.

En particular, el Teorema 2.17 nos dice que, si K es algebraicamente cerrado, la variedad más pequeña que contiene a $\pi_m(V)$, y por tanto también a $F(K^m)$, es $\mathbf{V}(I_m)$. ¿Qué ocurre en el caso de que el cuerpo K no sea algebraicamente cerrado?

Teorema 2.21 (Implicitación polinómica)**.** *Sea K un cuerpo infinito y $F : K^m \longrightarrow K^n$ la aplicación definida por la parametrización polinómica. Sea $I = \langle x_1 - f_1,\ldots,x_n - f_n\rangle \subset K[t_1,\ldots,t_m,x_1,\ldots,x_n]$ y sea I_m el m-ésimo ideal de eliminación. Entonces $\mathbf{V}(I_m)$ es la variedad afín más pequeña de K^n que contiene a $F(K^m)$.*

Demostración. Como acabamos de ver, si K es algebraicamente cerrado este resultado es un corolario inmediato del Teorema 2.17 (Teorema de Clausura). Veamos pues que ocurre cuando K no es algebraicamente cerrado.

Denotamos por $\overline{K}$ la clausura algebraica de K, y de esta forma $\mathbf{V}_{K^n}(I_m)$ denota la variedad en K y $\mathbf{V}_{\overline{K}^n}(I_m)$ denota la variedad en $\overline{K}$. Por la ecuación (2.1) sabemos que $F(K^m) = \pi_m(V) \subset \mathbf{V}_{K^n}(I_m)$. Sea $Z_K = \mathbf{V}_{K^n}(g_1,\ldots,g_s)$ una variedad de K^n tal que

$F(K^m) \subset Z_K$. Nuestro objetivo es demostrar que $\mathbf{V}_{K^n}(I_m)$ es la menor variedad afín que contiene a $F(K^m)$, es decir, que $\mathbf{V}_{K^n}(I_m) \subset Z_K$.

Como $F(K^m) \subset Z_K$, para todo $i \in \{1, \ldots, n\}$, se tiene que

$$g_i \circ F = g_i(f_1(t_1, \ldots, t_m), \ldots, f_n(t_1, \ldots, t_m)) \in K[t_1, \ldots, t_m]$$

es cero en todo punto de K^m, y como K es un cuerpo infinito, $g_i \circ F$ es el polinomio cero. Esto implica en particular, que $g_i \circ F$ también es el polinomio cero en $\overline{K}^m$, y que entonces los g_i se anulan en todo punto de $F(\overline{K}^m)$. De hecho $Z_{\overline{K}} = \mathbf{V}_{\overline{K}^n}(g_1, \ldots, g_s)$ es una variedad de $\overline{K}^n$ que contiene a $F(\overline{K}^m)$. Como el teorema es cierto para $\overline{K}$ por ser algebraicamente cerrado, tenemos que $\mathbf{V}_{\overline{K}^n}(I_m) \subset Z_{\overline{K}}$ en $\overline{K}^n$.

Si de esos conjuntos, solo tomamos las soluciones que están en K^n, es inmediato ver que $\mathbf{V}_{K^n}(I_m) \subset Z_K$, y así queda probado el teorema. □

Con este resultado ya estamos en condiciones de construír un *algoritmo para resolver el problema de implicitación en el caso de que la parametrización sea polinómica:*

Si tenemos nuestras variables definidas como: $x_i = f_i(t_1, \ldots, t_m), i \in \{1, \ldots, n\}$, consideramos el ideal $I = \langle x_1 - f_1, \ldots, x_n - f_n \rangle$ y hallamos una base de Groebner de dicho ideal respecto al orden lexicográfico, con $t_1 > \ldots > t_m > x_1 > \ldots > x_n$. El teorema de eliminación nos garantiza entonces que los elementos de la base de Groebner que no contienen a las variables $t_1, \ldots, t_m$ forman una base de I_m. En conclusión, esos elementos definen la variedad que buscamos de forma implícita.

2.3.2. Parametrización racional.

Para resolver el problema en el caso general nos falta analizar el caso de que la parametrización sea racional: Consideremos una parametrización de un subconjunto de K^n dado por una expresión de la forma

$$\begin{cases} x_1 & = \dfrac{p_1(t_1, \ldots, t_m)}{q_1(t_1, \ldots, t_m)} \\ \vdots & \vdots \\ x_n & = \dfrac{p_n(t_1, \ldots, t_m)}{q_n(t_1, \ldots, t_m)} \end{cases}$$

Donde $p_1, q_1, \ldots, p_n, q_n \in K[t_1, \ldots, t_m]$, y $q_1, \ldots, q_n$ son no nulos. Una primera idea para abordar este nuevo problema es eliminar los denominadores y utilizar el mismo método que en el caso de parametrizaciones polinómicas, considerando ahora las ecuaciones: $q_1 \cdot x_1 - p_1 = 0, \ldots, q_n \cdot x_n - p_n = 0$. Sin embargo este argumento no siempre funciona.

Ejemplo 2.22. Para ver un caso en el que intentar eliminar los denominadores con este método no nos sirve, consideremos la parametrización racional dada por:

$$x = \frac{u^3}{v^2}, \qquad y = \frac{v^2}{u^3}, \qquad z = u.$$

Es sencillo comprobar que cualquier punto de este tipo $(x, y, z) \in \mathbb{C}^3$ pertenece a la superficie $xy = 1$, esto es, que todos los puntos de la parametrización pertenecen a la variedad $\mathbf{V}(xy - 1)$. Veamos que ocurre si quitamos los denominadores y aplicamos el algoritmo dado por el Teorema 2.21: Consideramos el ideal que resulta quitando los denominadores,

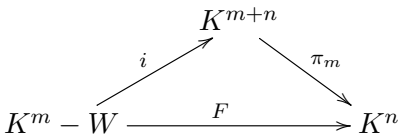
$$I = \langle u^3 - v^2 x, u^3 y - v^2, u - z \rangle \in K[u, v, x, y, z].$$

El segundo ideal de eliminación de I, considerando el orden lexicográfico, con $u > v > x > y > z$ es $I_2 = I \cap K[x, y, z] = \langle -z^3 + xyz^3 \rangle = \langle z^3 \cdot (xy - 1) \rangle$. Entonces $\mathbf{V}(I_2) = \mathbf{V}(xy - 1) \cup \mathbf{V}(z^3)$, y dado que la parametrización está contenida en $\mathbf{V}(xy - 1)$, esto nos indica que $\mathbf{V}(I_2)$ no es la menor variedad que contiene a la parametrización.

Uno de los fallos que tiene este modo de proceder es que en este caso las funciones $\frac{p_i}{q_i}$ pueden no estar definidas en todos los puntos de K^m. Para arreglar esto, podemos definir $W = \mathbf{V}(q_1 q_2 \cdots q_n) \subset K^m$. Como W es el conjunto de todos los puntos en los que alguno de los denominadores se anula, es evidente que el morfismo $F : K^m - W \longrightarrow K^n$, definido por

$$F(t_1, \ldots, t_m) = \left(\frac{p_1(t_1, \ldots, t_m)}{q_1(t_1, \ldots, t_m)}, \ldots, \frac{p_n(t_1, \ldots, t_m)}{q_n(t_1, \ldots, t_m)} \right)$$

sí que es una aplicación bien definida. Igual que antes, para resolver el problema de implicitación necesitamos encontrar la menor variedad afín que contenga a $F(K^m - W)$. Si, como antes, relacionamos esta aplicación con la aplicación grafo i y la proyección en las últimas n coordenadas π_m, definidas previamente, obtenemos el diagrama:



Si consideramos el ideal $I = \langle g_1 \cdot x_1 - f_1, \ldots, g_n \cdot x_n - f_n \rangle$, la variedad que define dicho ideal contiene a la imagen de la aplicación i: $i(K^m - W) \subset \mathbf{V}(I)$. Pero como vimos en el Ejemplo 2.22 esta variedad no siempre es la más pequeña que contiene a $i(K^m - W)$.

Para arreglar este problema, vamos a añadir una variable más a nuestro anillo de polinomios. Sea $q = q_1 q_2 \cdots q_n$ el producto de todos los denominadores de la parametrización racional, es decir, $W = \mathbf{V}(q)$. Consideramos ahora el ideal:

$$J = I \cup \langle 1 - qy \rangle = \langle q_1 \cdot x_1 - p_1, \ldots, q_n \cdot x_n - p_n, 1 - qy \rangle \subset K[y, t_1, \ldots, t_m, x_1, \ldots, x_n].$$

La ecuación que hemos añadido, $1 - qy = 0$, hace que los denominadores no se anulen. Ahora, para crear un diagrama similar al que teníamos en el caso inicial, necesitamos definir una nueva aplicación, $j : K^m - W \longrightarrow K^{1+m+n}$, dada por:

$$j(t_1, \ldots, t_m) = \left(\frac{1}{q(t_1, \ldots, t_m)}, t_1, \ldots, t_m, \frac{p_1(t_1, \ldots, t_m)}{q_1(t_1, \ldots, t_m)}, \ldots, \frac{p_n(t_1, \ldots, t_m)}{q_n(t_1, \ldots, t_m)} \right).$$

Lema 2.23. *Sean J el ideal y $j : K^m - W \longrightarrow K^{1+m+n}$ la aplicación que acabamos de definir. Entonces $j(K^m - W) = \boldsymbol{V}(J) \subset K^{1+m+n}$.*

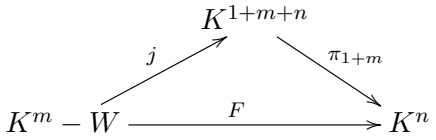
Demostración. Por las definiciones que acabamos de dar del ideal J y de la aplicación j, la inclusión $j(K^m - W) \subset \mathbf{V}(J)$ es inmediata.

Sea $(b, \lambda_1, \ldots, \lambda_m, a_1, \ldots, a_n) \in \mathbf{V}(J)$ un punto. Tenemos que demostrar que dicho punto está en la imagen de $K^m - W$ a través de la aplicación j. Igualando término a término el punto con la imagen de la aplicación, tenemos las siguientes igualdades:

$$b = \frac{1}{q(\lambda_1, \ldots, \lambda_m)},\ \lambda_1 = \lambda_1, \ldots, \lambda_m = \lambda_m,\ a_1 = \frac{p_1(\lambda_1, \ldots, \lambda_m)}{q_1(\lambda_1, \ldots, \lambda_m)}, \ldots, a_n = \frac{p_n(\lambda_1, \ldots, \lambda_m)}{q_n(\lambda_1, \ldots, \lambda_m)}.$$

La primera de estas igualdades es equivalente a que $1 - qy = 0$. Esto nos indica, además, que ninguno de los denominadores se anula en $(\lambda_1, \ldots, \lambda_m)$. Usando esto, las ecuaciones del ideal dadas por $q_i \cdot x_i - p_i = 0$ pueden resolverse con $x_i = \frac{p_i}{q_i}$, que es precisamente la expresión de la imagen de la coordenada $(1 + m + i)$-ésima a través de j, para todo $i \in \{1, \ldots, n\}$. Con esto queda claro que el punto pertenece a $\mathbf{V}(J)$ y queda probado el lema. □

Probado este resultado, la relación que hay ahora entre las aplicaciones es la siguiente:



Por lo que podemos descomponer la aplicación F como: $F = \pi_{1+m} \circ j$, y entonces:

$$F(K^m - W) = \pi_{1+m}(j(K^m - W)) = \pi_{1+m}(\mathbf{V}(J)). \tag{2.2}$$

Con esta igualdad, podemos resolver el problema de implicitación usando la teoría de la eliminación de forma análoga al caso en el que la parametrización era polinómica.

Teorema 2.24 (Implicitación racional)**.** *Sean K un cuerpo infinito y $F : K^m - W \longrightarrow K^n$ la función determinada por la parametrización racional. Sea además*

$$J = \langle x_1 q_1 - p_1, \ldots, x_n q_n - p_n, 1 - qy \rangle \subset K[y, t_1, \ldots, t_m, x_1, \ldots, x_n]$$

donde $q = q_1 q_2 \cdots q_n$*, y sea* $J_{1+m} = J \cap K[x_1, \ldots, x_n]$ *el* $(1+m)$*-ésimo ideal de eliminación para el orden lexicográfico determinado por* $y > t_1 > \ldots > t_m > x_1 > \ldots > x_n$*. Entonces* $\boldsymbol{V}(J_{m+1})$ *es la variedad afín más pequeña de* K^n *que contiene a* $F(K^m - W)$*.*

Demostración. Si K es un cuerpo algebraicamente cerrado este resultado es un corolario del Teorema 2.17 (Teorema de clausura).

Supongamos ahora que K es un cuerpo infinito no necesariamente algebraicamente cerrado. Sea $V = \mathbf{V}(J) \subset K^{1+m+n}$. Por (2.2), sabemos que $F(K^m - W) = \pi_{1+m}(V)$, y además se tiene la siguiente inclusión: $\pi_{1+m}(V) \subset \mathbf{V}_{K^n}(J_{1+m})$. Consideremos ahora una variedad $Z_K = \mathbf{V}(q_1, \ldots, q_s) \subset K^n$ que verifica que $F(K^m - W) \subset Z_K$. Tenemos que demostrar que $\mathbf{V}(J_{1+m}) \subset Z_K$.

Como $F(K^m - W) \subset Z_K$, para todo i se tiene que $g_i \circ F \in K(t_1, \ldots, t_m)$ es cero en todo punto de $K^m - W$. Si demostramos que $g_i \circ F$ es cero en $K(t_1, \ldots, t_m)$, la demostración se concluye con el mismo argumento que en el Teorema 2.21. Consideremos el polinomio $(g_i \circ F) \cdot q^r$ y veamos que es cero en todo punto $a \in K^{1+m+n}$: Si $a \in W$, tenemos que $q(a) = 0$, y si $a \in K^m - W$, como F solo actúa sobre las variables $t_1, \ldots, t_m$, $(g_i \circ F)(a) = 0$. Entonces $(g_i \circ F) \cdot q^r$ es el polinomio cero, y como el anillo de polinomios es un dominio y $q \neq 0$, entonces $g_i \circ F$ es necesariamente el polinomio cero, y la demostración se concluye entonces del mismo modo que en el Teorema 2.21. □

Capítulo 3

Aplicaciones de las bases de Groebner

3.1. Programación Lineal Entera.

Consideremos un problema de programación lineal entera puro, es decir, donde todos los coeficientes que aparezcan representen números enteros. Dicho problema podría plantearse de la forma siguiente:

mín / máx $\ell(\mathbf{A})$, $\mathbf{A}=(A_1,\ldots,A_n)\in\mathbb{Z}^n$ sujeto a:

$$\begin{array}{ccccccccc} a_{11}A_1 & + & a_{12}A_2 & + & \ldots & + & a_{1n}A_n & \leqslant & b_1 \\ a_{21}A_1 & + & a_{22}A_2 & + & \ldots & + & a_{2n}A_n & \leqslant & b_2 \\ \vdots & & \vdots & & \ddots & & \vdots & & \vdots \\ a_{m1}A_1 & + & a_{m2}A_2 & + & \ldots & + & a_{mn}A_n & \leqslant & b_m \end{array} \tag{3.1}$$

Donde $\ell : \mathbb{Z}^n \longrightarrow \mathbb{R}$ es una función lineal con coeficientes reales, $\mathbf{A}=(A_1,\ldots,A_n)$ son las variables, y los coeficientes a_{ij}, b_j son números enteros. Resolveremos únicamente el caso en el que las variables representen números enteros no negativos, es decir, $\mathbf{A}\in\mathbb{N}^n$, pero la forma de hallar la solución puede extenderse para resolver el problema con variables enteras.

Como máx $\ell(\mathbf{A})$ = -mín (-$\ell(\mathbf{A})$), nos restringiremos sin pérdida de generalidad al caso de minimizar funciones. Además, consideraremos únicamente restricciones de tipo $\leqslant$ ya que

$$a_{i1}A_1 + a_{i2}A_2 + \ldots + a_{in}A_n \geqslant b_i$$

es equivalente a

$$-a_{i1}A_1 - a_{i2}A_2 - \ldots - a_{in}A_n \leqslant -b_i,$$

por lo que todas las restricciones de tipo $\geqslant$ pueden ser sustituídas por restricciones equivalentes de tipo $\leqslant$. En conclusión, el problema que nos centraremos en resolver es el siguiente:

$$\begin{array}{lccccccccc} \text{mín} & c_1A_1 & + & c_2A_2 & + & \ldots & + & c_nA_n & & \\ \text{sujeto a :} & a_{11}A_1 & + & a_{12}A_2 & + & \ldots & + & a_{1n}A_n & \leqslant & b_1 \\ & a_{21}A_1 & + & a_{22}A_2 & + & \ldots & + & a_{2n}A_n & \leqslant & b_2 \\ & \vdots & & \vdots & & \ddots & & \vdots & & \vdots \\ & a_{m1}A_1 & + & a_{m2}A_2 & + & \ldots & + & a_{mn}A_n & \leqslant & b_m \end{array} \tag{3.2}$$

donde $\mathbf{A} = (A_1, \ldots, A_n) \in \mathbb{N}^n$, $a_{ij}, b_j \in \mathbb{Z}$, y $c_j \in \mathbb{R}$.

Llamaremos región factible relajada del problema (3.2) a los puntos $(A_1, \ldots, A_n) \in \mathbb{R}^n$ que verifican las restricciones, y región factible del problema (3.2) a los puntos de la región factible relajada tales que $(A_1, \ldots, A_n) \in \mathbb{N}^n$. Por último, para poder escribir el problema con restricciones de igualdad, procedemos como sigue:

Para cada restricción del tipo

$$a_{i1}A_1 + a_{i2}A_2 + \ldots + a_{in}A_n \leqslant b_i$$

consideramos la variable $\beta_i = b_i - (a_{i1}A_1 + a_{i2}A_2 + \ldots + a_{in}A_n) \geqslant 0$, y de esta forma podemos reescribir la restricción anterior como

$$a_{i1}A_1 + a_{i2}A_2 + \ldots + a_{in}A_n + \beta_i = b_i.$$

Estas variables β_i, denominadas variables de holgura, aparecen en la función objetivo con coeficiente nulo. Por tanto, todo problema de programación linear entera en $\mathbb{N}^n$ puede ser escrito en forma estándar como:

$$\begin{array}{lccccccccc} \text{mín} & c_1A_1 & + & c_2A_2 & + & \ldots & + & c_nA_n & & \\ s.a. : & a_{11}A_1 & + & a_{12}A_2 & + & \ldots & + & a_{1n}A_n & = & b_1 \\ & a_{21}A_1 & + & a_{22}A_2 & + & \ldots & + & a_{2n}A_n & = & b_2 \\ & \vdots & & \vdots & & \ddots & & \vdots & & \vdots \\ & a_{m1}A_1 & + & a_{m2}A_2 & + & \ldots & + & a_{mn}A_n & = & b_m \end{array} \tag{3.3}$$

donde $\mathbf{A} = (A_1, \ldots, A_n) \in \mathbb{N}^n$, $a_{ij}, b_j \in \mathbb{Z}$, y $c_j \in \mathbb{R}$.

Notemos que podemos suponer que todas las varibles $A_1, \ldots, A_n$ aparecen en al menos una de las desigualdades, es decir, que para cada j, los $a_{1j}, \ldots, a_{mj}$ no se anulan simultáneamente. En caso contrario la variable A_j no estaría sujeta a ninguna restricción salvo a la de pertenecer a $\mathbb{Z}$ y entonces, si el c_j correspondiente es positivo bastaría tomar $A_j = 0$ para minimizar la función y resolver el problema con una variable menos; mientras que si

c_j es negativo el problema no tendría, solución en general, pues la función $\ell(\mathbf{A})$ no tendría mínimo.

Ahora nos centraremos en convertir el problema (3.3) en un problema sobre ecuaciones polinómicas que posteriormente resolveremos usando bases de Groebner.

Estudiaremos primero el caso en el que a_{ij} y b_j son números naturales, y luego extenderemos el proceso al caso de coeficientes enteros.

Lo primero que debemos hacer es introducir una nueva variable z_i en cada restricción de (3.3), de modo que la nueva restricción de nuestro problema se escriba ahora como $z_i^{a_{i1}A_1+a_{i2}A_2+\cdots+a_{in}A_n} = z_i^{b_i}$, con $i \in \{1,\ldots,m\}$ o, más abreviadamente, como

$$\prod_{j=1}^{n} z_i^{a_{ij}A_j} = z_i^{b_i}, \text{ con } i \in \{1,\ldots,m\}. \tag{3.4}$$

Estas igualdades deben verificarse para todos los valores de z_i si $(A_1,\ldots,A_n)$ está en la región factible del problema (3.3). Multiplicando entre sí las m expresiones de (3.4) correspondientes a cada restricción obtenemos

$$\prod_{i=1}^{m}\left(\prod_{j=1}^{n} z_i^{a_{ij}A_j}\right) = \prod_{j=1}^{n}\left(\prod_{i=1}^{m} z_i^{a_{ij}}\right)^{A_j} = \prod_{i=1}^{m} z_i^{b_i}, \tag{3.5}$$

de esta igualdad podemos deducir el siguiente resultado:

Proposición 3.1. *Sea K un cuerpo y supongamos que estamos en las condiciones del problema (3.3). Sea $\varphi : K[w_1,\ldots,w_n] \longrightarrow K[z_1,\ldots,z_m]$ el K-homomorfismo de anillos determinado por:*

$$\varphi(w_j) = \prod_{i=1}^{m} z_i^{a_{ij}}, \text{ con } j \in \{1,\ldots,n\},$$

es decir, $\varphi(g(w_1,\ldots,w_n)) = g(\varphi(w_1),\ldots,\varphi(w_n))$. Entonces el punto $(A_1,\ldots,A_n)$ pertenece a la región factible del problema (3.3) si, y sólo si, $\varphi(w_1^{A_1}\cdots w_n^{A_n}) = z_1^{b_1}\cdots z_m^{b_m}$.

Demostración. $(A_1,\ldots,A_n)$ está en la región factible de (3.3) si, y sólo si

$$\prod_{j=1}^{n}\left(\prod_{i=1}^{m} z_i^{a_{ij}}\right)^{A_j} = \prod_{i=1}^{m} z_i^{b_i},$$

donde la igualdad se produce en el anillo $K[z_1,\ldots,z_m]$. Por la definición de φ, esta igualdad es equivalente a que

$$\prod_{j=1}^{n} (\varphi(w_j))^{A_j} = \prod_{i=1}^{m} z_i^{b_i},$$

y dada esta igualdad, el resultado es inmediato:

$$\varphi(w_1^{A_1}\cdots w_n^{A_n}) = \varphi(w_1)^{A_1}\cdots\varphi(w_n)^{A_n} = \prod_{j=1}^{n}(\varphi(w_j))^{A_j} = \prod_{i=1}^{m} z_i^{b_i} = z_1^{b_1}\cdots z_m^{b_m}. \qquad \square$$

Notemos que φ no es, en general, sobreyectiva. Por la forma de definir la aplicación φ, es claro que los polinomios de $K[z_1, \ldots, z_m]$ que son imagen por φ de algún polinomio en $K[w_1, \ldots, w_n]$ son aquellos que es pueden expresar como combinación de los polinomios $f_j := \prod_{i=1}^{m} z_i^{a_{ij}} = \varphi(w_j)$. Es decir, la imagen de φ es el subanillo $K[f_1, \ldots, f_n]$ de $K[z_1, \ldots, z_n]$

En lo sucesivo, por simplicidad, escribiremos $\boldsymbol{z}$ para denotar al conjunto de variables $z_1, \ldots, z_m$, y $\boldsymbol{w}$ para $w_1, \ldots, w_n$. Primero, introduciremos el K-homomorfismo de anillos ψ, que extiende al K-homomorfismo φ que hemos definido previamente:

$$\psi : K[\boldsymbol{z}, \boldsymbol{w}] \longrightarrow K[\boldsymbol{z}]$$

definido por:

$$\psi(z_i) = z_i, \text{ con } i \in \{1, \ldots, m\}, \qquad \psi(w_j) = \varphi(w_j) = f_j, \text{ con } j \in \{1, \ldots, n\},$$

es decir, $\psi(g(z_1, \ldots, z_m, w_1, \ldots, w_n)) = g(\psi(z_1), \ldots, \psi(z_m), \psi(w_1), \ldots, \psi(w_n))$, considerado para los polinomios $f_1(\boldsymbol{z}), \ldots, f_n(\boldsymbol{z}) \in K[\boldsymbol{z}]$ que acabamos de definir. Aunque los siguientes resultados estén enunciados para polinomios $f_1, \ldots, f_n$ arbitrarios, tendrá un interés particular el caso de considerar precisamente estos polinomios.

Lema 3.2. *Sean polinomios arbitrarios $f_1(\boldsymbol{z}), \ldots, f_n(\boldsymbol{z}) \in K[\boldsymbol{z}]$. En las condiciones anteriores, sea $I = \langle f_1 - w_1, \ldots, f_n - w_n \rangle \subset K[\boldsymbol{z}, \boldsymbol{w}]$. Entonces* $\ker(\psi) = I$.

Demostración. Probaremos por separado las dos inclusiones. En primer lugar, sea $h \in I$. Podemos escribir $h = h_1(f_1 - w_1) + \ldots + h_n(f_n - w_n)$, con $h_j \in K[\boldsymbol{z}, \boldsymbol{w}]$. Aplicando ψ obtenemos: $\psi(h) = \psi(h_1)[\psi(f_1) - \psi(w_1)] + \ldots + \psi(h_n)[\psi(f_n) - \psi(w_n)]$. Dado que $\psi(f_j) = f_j$ por ser combinación de las z_i, y $\psi(w_j) = f_j$, tenemos que $\psi(h) = 0$ y entonces $h \in \ker(\psi)$.

Para ver la otra inclusión, sea $f \in K[\boldsymbol{z}, \boldsymbol{w}]$ tal que $\psi(f) = 0$. Si consideramos el orden lexicográfico, con $w_1 > \ldots > w_n > z_1 > \ldots > z_m$, y dividimos f entre los polinomios $\{-w_1 + f_1, \ldots, -w_n + f_n\}$, obtenemos la siguiente expresión:

$$f(w_1, \ldots, w_n, z_1, \ldots, z_m) = \sum_{j=1}^{n} h_j(f_j(\boldsymbol{z}) - w_j) + r.$$

Además, como los monomios líderes son $w_1, \ldots, w_n$, el resto r no depende de dichas variables, por lo que $r = r(\boldsymbol{z})$, y además $\psi(r(\boldsymbol{z})) = r(\boldsymbol{z})$. Aplicando ψ tenemos que:

$$0 = \psi(f) = \sum_{j=1}^{n} \psi(h_j)[\psi(f_j(\boldsymbol{z})) - \psi(w_j)] + \psi(r(\boldsymbol{z})) = \psi(r(\boldsymbol{z})).$$

De aquí deducimos que $r(\boldsymbol{z}) = 0$ y entonces $f \in I$. □

Proposición 3.3. *Consideremos $f_1, \ldots, f_n \in K[\boldsymbol{z}]$ polinomios arbitrarios. Sea G una base de Groebner para el ideal*

$$I = \langle f_1 - w_1, \ldots, f_n - w_n \rangle \subset K[\boldsymbol{z}, \boldsymbol{w}]$$

respecto a un orden monomial en $K[\boldsymbol{z}, \boldsymbol{w}]$ en el que todo monomio que contenga a alguna de las variables z_i es mayor que cualquier monomio que solo contenga a las variables w_j, y sea $f \in K[\boldsymbol{z}]$. Si denotamos $r = \overline{f}^G$ entonces:

- *$f \in K[f_1, \ldots, f_n]$ si, y sólo si, $r = \overline{f}^G \in K[\boldsymbol{w}]$.*
- *Si $f \in K[f_1, \ldots, f_n]$ entonces $f = r(f_1, \ldots, f_n)$ nos da una expresión de f en función de los polinomios $f_1, \ldots, f_n$.*
- *Si $f, f_1, \ldots, f_n$ son monomios y $f \in K[f_1, \ldots, f_n]$, entonces $r \in K[\boldsymbol{w}]$ también es un monomio.*

Demostración. Sea ψ el homomorfismo de anillos que hemos definido anteriormente, y sea $G = \{g_1, \ldots, g_t\}$. Supongamos que $r = \overline{f}^G \in K[\boldsymbol{w}]$. Aplicamos el algoritmo de la división para dividir el polinomio f por $\{g_1, \ldots, g_t\}$ y obtenemos

$$f = h_1^{'} g_1 + \ldots h_t^{'} g_t + r,$$

con $h_1^{'}, \ldots, h_t^{'} \in K[\boldsymbol{z}, \boldsymbol{w}]$. Teniendo en cuenta que $\langle f_1 - w_1, \ldots, f_n - w_n \rangle = \langle g_1, \ldots, g_t \rangle$, podemos reescribir f como

$$f = h_1(f_1 - w_1) + \ldots + h_n(f_n - w_n) + r.$$

Aplicando el homomorfismo ψ obtenemos que

$$f = \psi(f) = \psi(h_1[f_1 - w_1] + \ldots + h_n[f_n - w_n] + r) =$$

$$= \psi(h_1)[\psi(f_1) - \psi(w_1)] + \ldots + \psi(h_n)[\psi(f_n) - \psi(w_n)] + \psi(r) = \psi(r),$$

y como $r \in K[\boldsymbol{w}], \psi(r)$ se puede expresar en función de los polinomios $f_1, \ldots, f_n$, de forma que

$$f = \psi(r) = r(f_1, \ldots, f_n) \in K[f_1, \ldots, f_n].$$

Supongamos ahora $f \in K[f_1, \ldots, f_n]$, es decir, que podemos escribir $f = g(f_1, \ldots, f_n)$. Entonces cada monomio de f es también un elemento de $K[f_1, \ldots, f_n]$, y puede escribirse como

$$f_1^{A_1} \cdots f_n^{A_n} = (w_1 + (f_1 - w_1))^{A_1} \cdots (w_n + (f_n - w_n))^{A_n} =$$

$$= w_1^{A_1} \cdots w_n^{A_n} + B_1(f_1 - w_1) + \ldots + B_n(f_n - w_n)$$

para ciertos $B_1, \ldots, B_n \in K[\boldsymbol{z}, \boldsymbol{w}]$, luego nuestro polinomio f, que es una suma de monomios de este tipo, podrá expresarse como

$$f = g(f_1, \ldots, f_n) = g(w_1, \ldots, w_n) + C_1(f_1 - w_1) + \ldots + C_n(f_n - w_n),$$

con $C_1, \ldots, C_n \in K[\boldsymbol{z}, \boldsymbol{w}]$, y por tanto

$$r = \overline{f}^G = \overline{g'(w_1, \ldots, w_n)}^G + \overline{\sum_{j=1}^{n} C_j(f_j - w_j)}^G = \overline{g'(w_1, \ldots, w_n)}^G.$$

Ahora, dado que G es una base de Groebner de I, y $g'(w_1, \ldots, w_n) \in K[\boldsymbol{w}]$, el resto al dividirlo por G también estará en $K[\boldsymbol{w}]$.

Finalmente, si $f, f_1, \ldots, f_n$ son monomios y $f \in K[f_1, \ldots, f_n]$ tenemos que los elementos de G serán combinación lineal de a lo sumo dos monomios, pues los elementos que generan I son resta de dos monomios, $f_i - w_i$, y al realizar sizigias entre sus elementos los términos principales de cada uno de ellos se cancelan, quedando de nuevo dos monomios. Al aplicar el algoritmo de la división para dividir el monomio f entre elementos que son suma de dos monomios, el resto tendrá a lo sumo un monomio, ya que uno de los monomios de los divisores se cancela con el monomio al que le estamos aplicando el algoritmo. Con esto quedan probados todos los enunciados de la proposición. □

Corolario 3.4. *Sea $f = z_1^{b_1} \cdots z_m^{b_m} \in K[\boldsymbol{z}]$. Si $f \in K[f_1, \ldots, f_n]$, entonces $\overline{f}^G \in K[\boldsymbol{w}]$. Además, si f está en la imagen de la aplicación φ que hemos definido anteriormente, entonces debe ser imagen de algún monomio $w_1^{A_1} \cdots w_n^{A_n}$.*

Antes de enunciar el resultado que resolverá el problema (3.3), necesitamos definir un tipo de órdenes monomiales con dos propiedades interesantes, que serán precisamente los que utilizaremos para resolver los problemas de programación lineal entera usando bases de Groebner.

Definición 3.5. Un orden monomial en $K[\boldsymbol{z}, \boldsymbol{w}]$ se dice que está adaptado al problema de programación lineal entera (3.3) si verifica:

- *Eliminación de las variables $\boldsymbol{w}$:* para todo monomio $\boldsymbol{x}^{\boldsymbol{\alpha}}$ que contenga alguna de las variables z_i, y todo monomio $\boldsymbol{x}^{\boldsymbol{\beta}}$ que solo contenga a las variables w_j, se tiene que $\boldsymbol{x}^{\boldsymbol{\alpha}} > \boldsymbol{x}^{\boldsymbol{\beta}}$.
- *Compatibilidad con ℓ:* Sean $\mathbf{A}(A_1, \ldots, A_n)$ y $\mathbf{A}'(A_1', \ldots, A_n') \in \mathbb{N}^n$. Si los monomios $\boldsymbol{w}^{\mathbf{A}} = w_1^{A_1} \cdots w_n^{A_n}$ y $\boldsymbol{w}^{\mathbf{A}'} = w_1^{A_1'} \cdots w_n^{A_n'}$ satisfacen que $\varphi(\boldsymbol{w}^{\mathbf{A}}) = \varphi(\boldsymbol{w}^{\mathbf{A}'})$ y también que $\ell(\mathbf{A}) > \ell(\mathbf{A}')$, entonces $\boldsymbol{w}^{\mathbf{A}} > \boldsymbol{w}^{\mathbf{A}'}$.

Ahora sí, estamos en condiciones de resolver el problema de programación lineal entera (3.3) de forma general.

Teorema 3.6. *Consideremos un problema de programación lineal entera en forma estándar como problema (3.3), con los coeficientes $a_{ij}, b_j \in \mathbb{N}$. Sea $\leq$ un orden monomial adaptado a dicho problema, y sea $f_j = \prod_{i=1}^{m} z_i^{a_{ij}}$, con $j \in \{1, \ldots, n\}$. Consideremos el ideal*

$$I = \langle f_1 - w_1, \ldots, f_n - w_n \rangle \subset K[\boldsymbol{z}, \boldsymbol{w}]$$

y sea G una base de Groebner de I respecto al orden monomial $\leq$. Entonces si el monomio $f = z_1^{b_1} \cdots z_m^{b_m} \in K[f_1, \ldots, f_n]$, el resto $\overline{f}^G \in K[\boldsymbol{w}]$, que también es un monomio, nos proporcionará una solución de (3.3).

Demostración. Está claro que, si $f = z_1^{b_1} \cdots z_m^{b_m} \in K[f_1, \ldots, f_n]$, entonces por lo visto anteriormente existe un punto $(A_1, \ldots, A_n) \in \mathbb{N}^n$ tal que:

$$f = z_1^{b_1} \cdots z_m^{b_m} = \varphi(w_1^{A_1} \cdots w_n^{A_n}) = \varphi(w_1)^{A_1} \cdots \varphi(w_n)^{A_n} = f_1^{A_1} \cdots f_n^{A_n} \in K[f_1, \ldots, f_n]$$

y por tanto $\overline{f}^G = w_1^{A_1} \cdots w_n^{A_n} \in K[\boldsymbol{w}]$ es un punto factible $(A_1, \ldots, A_n)$ en virtud de las Proposiciones 3.1 y 3.3. Nuestro objetivo ahora es demostrar que ese punto $(A_1, \ldots, A_n)$ es óptimo.

Supongamos que $\overline{f}^G = w_1^{A_1} \cdots w_n^{A_n} = \boldsymbol{w}^{\mathbf{A}}$, con $\varphi(\boldsymbol{w}^{\mathbf{A}}) = f$, pero que $(A_1, \ldots, A_n)$ no es un punto óptimo para (3.3). Esto quiere decir que existe un punto $\mathbf{A}'(A_1', \ldots, A_n') \neq \mathbf{A}$ tal que $\varphi(\boldsymbol{w}^{\mathbf{A}'}) = f$ y $\ell(\mathbf{A}) > \ell(\mathbf{A}')$. Como el orden monomial que hemos escogido es adaptado a nuestro problema de programación lineal, esta última desigualdad implica que $\boldsymbol{w}^{\mathbf{A}} > \boldsymbol{w}^{\mathbf{A}'}$. Si definimos $h = \boldsymbol{w}^{\mathbf{A}} - \boldsymbol{w}^{\mathbf{A}'} \in K[\boldsymbol{w}]$, tenemos que

$$\varphi(h) = \varphi(\boldsymbol{w}^{\mathbf{A}} - \boldsymbol{w}^{\mathbf{A}'}) = \varphi(\boldsymbol{w}^{\mathbf{A}}) - \varphi(\boldsymbol{w}^{\mathbf{A}'}) = f - f = 0$$

y por tanto, el Lema 3.2 nos indica que el polinomio h pertenece a I. Esto implica que $\boldsymbol{w}^{\mathbf{A}} = \text{LT}(h) \in \text{LT}(I)$, pero por otro lado $\text{LT}(h) = \boldsymbol{w}^{\mathbf{A}} = \overline{f}^G$ y esto implica que $\text{LT}(h) \notin \text{LT}(I)$, lo cual es una contradicción. Por tanto el punto $(A_1, \ldots, A_n)$ sí es óptimo. □

Este teorema nos proporciona un algoritmo para resolver el problema (3.3), cuando $a_{ij}, b_j \in \mathbb{N}$, en caso de que este tenga solución; y para determinar cuándo no la tiene: Con la notación previa, si $g = \overline{f}^G \in K[\boldsymbol{w}]$, entonces una solución del problema viene dada por el vector formado por los exponentes de g, mientras que si $g \notin K[\boldsymbol{w}]$ el problema no tiene solución.

Ahora vamos a ocuparnos del caso en el que $a_{ij}, b_j \in \mathbb{Z}$. Para resolverlo una primera idea es extender el algoritmo que acabamos de diseñar para el caso de que los coeficientes a_{ij}, b_j

sean no negativos. El problema que nos encontramos es que ahora las variables z_i pueden tener exponente negativo, y por tanto las expresiones $\prod_{i=1}^{m} z_i^{b_i}$ y $\prod_{i=1}^{m}\left(\prod_{j=1}^{n} z_i^{a_{ij}A_j}\right)$ pueden no ser elementos del anillo de polinomios $K[z_1,\ldots,z_m]$.

Para resolver este problema vamos a hacer algo muy similar a lo que hicimos cuando queríamos extender el algoritmo del problema de implicitación polinómica al problema de implicitación racional: Consideramos una nueva variable t, el anillo de polinomios $K[z_1,\ldots,z_m,t]$ y el ideal $J=\langle tz_1\cdots z_m-1\rangle\subset K[\boldsymbol{z},t]$.

Lo que haremos será adaptar los resultados que hemos visto para el caso de coeficientes no negativos, en el que trabajábamos con el anillo de polinomios $K[\boldsymbol{z}]$. Sin embargo, en este caso tendremos que trabajar con el anillo cociente

$$\frac{K[z_1,\ldots,z_m,t]}{\langle tz_1\cdots z_m-1\rangle}, \tag{3.6}$$

donde la igualdad $tz_1\cdots z_m-1=0$ nos indica que podemos pensar en la variable t como el producto de las variables $z_1^{-1}\cdots z_m^{-1}$.

Si reescribimos los coeficientes de la forma siguiente

$$(a_{1j},\ldots,a_{mj})=(a'_{1j},\ldots,a'_{mj})+\alpha_j(-1,\ldots,-1) \text{ para } j=1,\ldots,n,$$

$$(b_1,\ldots,b_m)=(b'_1,\ldots,b'_m)+\beta(-1,\ldots,-1),$$

con $a'_{ij},b'_i,\alpha_j,\beta\in\mathbb{N}$ para todo i y todo j, obtenemos las siguientes expresiones en el anillo cociente (3.6) para $j=1,\ldots,n$:

$$\prod_{i=1}^{m} z_i^{a_{ij}}=\prod_{i=1}^{m} z_i^{a'_{ij}-\alpha_j}=\prod_{i=1}^{m} z_i^{a'_{ij}}z_i^{-\alpha_j}=\left(\prod_{i=1}^{m} z_i^{-\alpha_j}\right)\left(\prod_{i=1}^{m} z_i^{a'_{ij}}\right)=t^{\alpha_j}\prod_{i=1}^{m} z_i^{a'_{ij}},$$

$$\prod_{i=1}^{m} z_i^{b_i}=\prod_{i=1}^{m} z_i^{b'_i-\beta}=\prod_{i=1}^{m} z_i^{b'_i}z_i^{-\beta}=\left(\prod_{i=1}^{m} z_i^{-\beta}\right)\left(\prod_{i=1}^{m} z_i^{b_i}\right)=t^{\beta}\prod_{i=1}^{m} z_i^{b'_i}.$$

Entonces, podemos reescribir la ecuación (3.5), adaptándola a las nuevas expresiones que tenemos para las restricciones en el anillo cociente (3.6), como:

$$\prod_{j=1}^{n}\left(t^{\alpha_j}\prod_{i=1}^{m} z_i^{a'_{ij}}\right)^{A_j}=t^{\beta}\prod_{i=1}^{m} z_i^{b'_i}$$

A la vista de esta igualdad, podemos adaptar la Proposición 3.1 al caso en el que nos encontramos. Esta proposición nos da una condición inequívoca para determinar nuestro conjunto de puntos factibles.

Proposición 3.7. *Sea K un cuerpo y supongamos que nos encontramos en las condiciones que acabamos de ver, siendo $J = \langle tz_1 \cdots z_m - 1\rangle \subset K[\boldsymbol{z}, t]$. Definimos el homomorfismo de anillos $\tilde{\varphi} : K[\boldsymbol{w}] \longrightarrow \dfrac{K[z_1, \ldots, z_m, t]}{J}$ como:*

$$\tilde{\varphi}(w_j) = \left(t^{\alpha_j} \prod_{i=1}^{m} z_i^{a'_{ij}} \right) + J,$$

$$\tilde{\varphi}(g(w_1, \ldots, w_n)) = g(\varphi(w_1), \ldots, \varphi(w_n)) + J,$$

donde $\varphi : K[\boldsymbol{w}] \longrightarrow K[\boldsymbol{z}, t]$ es el homomorfismo equivalente a $\tilde{\varphi}$ pero sin cocientar módulo J. Entonces $(A_1, \ldots, A_n)$ pertenece a la región factible de (3.3) si, y sólo si,

$$\left(\varphi(w_1^{A_1} \cdots w_n^{A_n})\right) + J = \left(t^{\beta} z_1^{b'_1} \cdots z_m^{b'_m} \right) + J.$$

Demostración. Por la Proposición 3.1, $(A_1, \ldots, A_n)$ está en la región factible de (3.3) si, y sólo si

$$\prod_{j=1}^{n} \left(\prod_{i=1}^{m} z_i^{a_{ij}} \right)^{A_j} = \prod_{i=1}^{m} z_i^{b_i},$$

que ya hemos visto que se corresponde en el anillo cociente con

$$\prod_{j=1}^{n} \left(t^{\alpha_j} \prod_{i=1}^{m} z_i^{a'_{ij}} \right)^{A_j} = t^{\beta} \prod_{i=1}^{m} z_i^{b'_i}.$$

Como $\tilde{\varphi}(w_j) = \left(t^{\alpha_j} \prod_{i=1}^{m} z_i^{a'_{ij}} \right) + J$, tomando clases de equivalencia, llegamos a la igualdad que nos garantiza que se verifican las restricciones:

$$\left(\prod_{j=1}^{n} (\varphi(w_j))^{A_j} \right) + J = \left(\varphi(w_1)^{A_1} \cdots \varphi(w_n)^{A_n}\right) + J =$$

$$= \left(\varphi(w_1^{A_1} \cdots w_n^{A_n})\right) + J = \left(t^{\beta} z_1^{b'_1} \cdots z_m^{b'_m} \right) + J = \left(t^{\beta} \prod_{i=1}^{m} z_i^{b'_i} \right) + J. \qquad \square$$

Igual que en el caso de coeficientes no negativos, volvemos a definir los polinomios

$$f_j = t^{\alpha_j} \prod_{i=1}^{m} z_i^{a'_{ij}} \in K[z_1, \ldots, z_m, t]$$

de modo que la imagen por φ de $K[w_1, \ldots, w_n]$ será el conjunto de polinomios de (3.6) que podamos expresar como polinomios en $f_1, \ldots, f_n$. Con esto, podemos simplificar la expresión del homomorfismo $\tilde{\varphi}$:

$$\tilde{\varphi}(w_j) = f_j + J.$$

El siguiente resultado, similar al de la Proposición 3.3, está enunciado para polinomios arbitrarios. Al igual que en el problema de coeficientes enteros no negativos, tendrá especial interés para la resolución del problema de programación lineal considerar los f_j que acabamos de definir.

Proposición 3.8. *Consideremos polinomios arbitrarios $f_1, \ldots, f_n \in K[\boldsymbol{z}, t]$, y un orden monomial en el que todo monomio que contenga a alguna de las variables z_i, t es mayor que aquel en el que solo aparezcan las variables w_j. Sea G una base de Groebner para el ideal $I = \langle tz_1 \cdots z_m - 1, f_1 - w_1, \ldots, f_n - w_n \rangle \subset K[\boldsymbol{z}, t, \boldsymbol{w}]$ y sea $f \in K[\boldsymbol{z}, t]$. Si denotamos $g = \overline{f}^G$, entonces:*

- *Existe $f' \in K[\boldsymbol{w}]$ tal que $\tilde{\varphi}(f') = [f] \in \frac{K[z_1,\ldots,z_m,t]}{J}$ si, y sólo si, $g \in K[\boldsymbol{w}]$.*
- *Si $f, f_1, \ldots, f_n$ son monomios, y $[f]$ está en la imagen por $\tilde{\varphi}$, entonces g también es un monomio de $K[\boldsymbol{w}]$.*

La demostración de este resultado se puede consultar en [9]. Probado esto, tenemos un resultado análogo al Teorema 3.6 que resuelve el problema de programación lineal entera con coeficientes enteros. Lo que nos dice dicho resultado es que si consideramos un orden monomial adaptado al problema (3.3) tenemos que:

Si $[f] = [z_1^{b_1'} \cdots z_m^{b_m'}] \in \tilde{\varphi}(K[w_1, \ldots, w_n])$, entonces el monomio $\overline{f}^G \in K[w_1, \ldots, w_n]$ proporciona una solución al problema 3.3 con coeficientes enteros. En caso contrario, el problema no tiene solución.

3.2. Teoría de grafos.

Un grafo $\mathcal{G}$ no dirigido se define de forma general mediante un conjunto finito de vértices $V_\mathcal{G}$, un conjunto finito de aristas $E_\mathcal{G}$, y una relación que asigna cada arista, e, a exactamente dos vértices, i, j, no necesariamente distintos. En el caso de que i y j sean iguales diremos que la arista e es un lazo. En general consideraremos únicamente grafos simples, esto es, sin lazos y sin aristas múltiples, y diremos que dos vértices i, j son adyacentes si existe una arista que los relacione.

Podemos ilustrar un grafo $\mathcal{G} = (V_\mathcal{G}, E_\mathcal{G})$ con un diagrama, asignando a cada vértice un punto en el plano y a cada arista una curva continua que no se corte a sí misma y cuyos extremos sean los puntos de los vértices a los que está asociada. Si existe un diagrama en el cual las aristas de $\mathcal{G}$ no se corten en más puntos que en los vértices, diremos que el grafo $\mathcal{G}$ es un grafo plano. Además, si cada par de vértices de un grafo $\mathcal{G}$ están conectados mediante una unión de aristas se dice que el grafo $\mathcal{G}$ es conexo. En caso contrario diremos que $\mathcal{G}$ es disconexo.

Definición 3.9. Sea $\mathcal{G} = (V_\mathcal{G}, E_\mathcal{G})$ un grafo general, con conjunto de vértices $V_\mathcal{G}$ y conjunto de aristas $E_\mathcal{G}$. Una q-coloración propia de $\mathcal{G}$ es una función

$$c : V_\mathcal{G} \longrightarrow C$$

de $V_\mathcal{G}$ en un conjunto C de cardinalidad q, tal que $c(i) \neq c(j)$ para todo par $(i, j) \in E_\mathcal{G}$. Diremos que el grafo $\mathcal{G}$ es q-coloreable si admite una q-coloración propia, y llamaremos color a cada elemento del conjunto C.

Es decir, en una q-coloración propia de un grafo no se admite que dos vértices adyacentes estén coloreados con el mismo color.

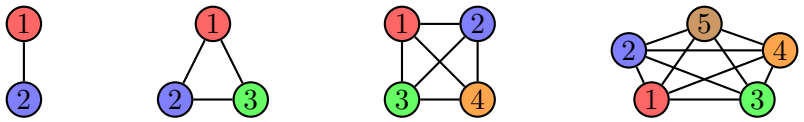
Notemos que, para cualquier grafo $\mathcal{G}$, cualquier coloración $c : V_\mathcal{G} \longrightarrow C$ induce una relación de equivalencia en el conjunto de vértices $V_\mathcal{G}$ en función del color, de manera que dos vértices i, j están relacionados si $c(i) = c(j)$.

De esta forma, cada color determina una clase de equivalencia, y basándonos en la partición inducida en el conjunto de vértices por esta relación, diremos que dos q-coloraciones propias son distintas cuando inducen particiones distintas en el conjunto de vértices $V_\mathcal{G}$. Más formalmente:

Definición 3.10. Un grafo $\mathcal{G} = (V_\mathcal{G}, E_\mathcal{G})$ es q-coloreable de manera única si existe una única q-coloración propia salvo permutaciones de colores.

Definición 3.11. Si $\mathcal{G}$ es un grafo q-coloreable pero no es k-coloreable para ningún númer natural $k < q$, diremos que q es el número cromático de $\mathcal{G}$.

Ejemplo 3.12. El número cromático de un grafo completo de n vértices es n. A continuación se muestran coloraciones de los grafos completos de 2, 3, 4 y 5 nodos:



El procedimiento para decidir si un grafo es q-coloreable con el uso de bases de Groebner es sistemático:

Definición 3.13. Sea $\mathcal{G}$ un grafo simple y no dirigido, con vértices $V_{\mathcal{G}} = \{1, \ldots, n\}$ y aristas $E_{\mathcal{G}}$. Llamaremos ideal de q-coloración del grafo $\mathcal{G}$ al ideal $I_{\mathcal{G},q} \subset \mathbb{C}[x_1, \ldots, x_n]$ generado por

$$x_i^q - 1, \text{ para todo } i \in V_{\mathcal{G}},$$

$$x_i^{q-1} + x_i^{q-2}x_j + \ldots + x_i x_j^{q-2} + x_j^{q-1} \text{ para todo } (i,j) \in E.$$

Lema 3.14. *$\mathbf{V}(I_{\mathcal{G},q}) \subset \mathbb{C}^n$ está formado por todas las q-coloraciones de $\mathcal{G}$. En este caso, consideramos que el conjunto de colores son las raíces q-ésimas de la unidad.*

Demostración. La variedad $\mathbf{V}(I_{\mathcal{G},q})$ está formada por los puntos de $\mathbb{C}^n$ que anulan todas las ecuaciones de polinomios de $I_{\mathcal{G},q}$ igualados a cero.

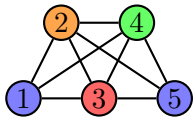
El polinomio $x_i^q - 1$ se anula si, y sólo si, el vértice i es una raíz q-ésima de la unidad, es decir, un color.

Además, los polinomios $x_i^{q-1} + x_i^{q-2}x_j + \ldots + x_i x_j^{q-2} + x_j^{q-1}$ serán cero únicamente si los vértices i y j tienen colores distintos, ya que

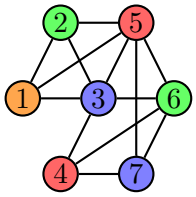
$$x_i^{q-1} + x_i^{q-2}x_j + \ldots + x_i x_j^{q-2} + x_j^{q-1} = \frac{(x_i^q - 1) - (x_j^q - 1)}{x_i - x_j}. \qquad \square$$

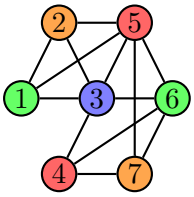
De esta forma, tenemos un criterio para decir cuando un grafo es q-coloreable. Este lema nos dice además que, si $\mathbf{V}(I_{\mathcal{G},q}) = \varnothing$, entonces el grafo $\mathcal{G}$ no admite ninguna q-coloración propia. Por otra parte, $\mathbf{V}(I_{\mathcal{G},q}) \neq \varnothing$ nos indica que existe al menos una q-coloración propia de nuestro grafo $\mathcal{G}$, pero no nos dice si esta coloración es única, ni cuántas existen.

Ejemplo 3.15. Veamos a continuación un grafo que admite una única 4-coloración y otro que admite más de una:



$\mathcal{G}_1$





$\mathcal{G}_2$

Los ideales de 4-coloración en cada uno de los grafos son los siguientes. En el caso del grafo $\mathcal{G}_1$ el conjunto de aristas es

$$E_1 = \{(1,2),(1,3),(1,4),(2,3),(2,4),(2,5),(3,4),(3,5),(4,5)\},$$

mientras que en el caso del grafo $\mathcal{G}_2$ el conjunto de aristas es

$$E_2 = \{(1,2),(1,3),(1,5),(2,3),(2,5),(3,4),(3,5),(3,6),(4,6),(4,7),(5,6),(5,7),(6,7)\}.$$

Siguiendo esta notación, los generadores de los ideales de 4-coloración de los grafos $\mathcal{G}_k$, para $k \in \{1,2\}$, son:

$$x_i^4 - 1, \text{ para todo } i \in V_k,$$

$$x_i^3 + x_i^2 x_j + x_i x_j^2 + x_j^3 \text{ para todo } (i,j) \in E_k.$$

Donde V_k es el conjunto de nodos de cada grafo: $V_1 = \{1,2,3,4,5\}, V_2 = \{1,2,3,4,5,6,7\}$.

A la vista del ejemplo anterior surge la siguiente cuestión: ¿Podemos saber si un grafo dado posee una única q-coloración? La respuesta es afirmativa si consideramos un conjunto apropiado de polinomios. A continuación detallamos quienes son esos polinomios.

Sea γ una q-coloración del grafo $\mathcal{G}$ de n vértices que usa los q colores, y supongamos que los q últimos vértices tienen cada uno un color distinto. Usaremos las variables $x_1, \ldots, x_{n-q}$ para los $n-q$ primeros vértices y las variables $y_1, \ldots, y_q$ para los q últimos.

Consideremos los polinomios $g_1, \ldots, g_n$ definidos por:

- $y_q^q - 1$.
- $h_j(y_j, \ldots, y_q) = \sum_{\alpha_j + \ldots, + \alpha_q = j} y_j^{\alpha_j} \cdots y_q^{\alpha_q}$, con $j = 1, \ldots, q-1$.
- $x_i + y_2 + \ldots + y_q$, si $\text{color}(x_i) = \text{color}(y_1)$.
- $x_i - y_j$, si $\text{color}(x_i) = \text{color}(y_j)$, si $j \geqslant 2$.

Usando los polinomios que acabamos de definir sí que es posible determinar cuando un grafo es q-coloreable de forma única.

Teorema 3.16. *Dado un grafo $\mathcal{G}$, sea $I_{\mathcal{G},q}$ su ideal de q-coloración. Consideremos las variables $x_1, \ldots, x_{n-q}, y_1, \ldots, y_q$ y los polinomios $g_1, \ldots, g_n$ que hemos definido anteriormente. Entonces los siguientes resultados son equivalentes:*

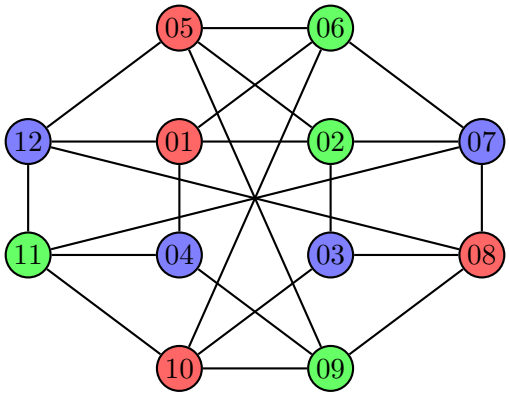
i $\mathcal{G}$ *es q-coloreable de manera única.*

ii $g_1, \ldots, g_n \in I_{\mathcal{G},q}$.

iii $\{g_1, \ldots, g_n\}$ *es la base de Groebner reducida de* $I_{\mathcal{G},q}$ *respecto al orden lexicográfico con* $x_1 > \ldots > x_{n-q} > y_1 > \ldots > y_q$.

La demostración de este resultado puede consultarse en [7].

Ejemplo 3.17. Dado el grafo $\mathcal{G}$ siguiente,



Las variables y_1, y_2 e y_3 son las asociadas a los nodos $10, 11$ y 12 respectivamente. Los polinomios $g_1, \ldots, g_n$ que acabamos de definir, asociados al grafo $\mathcal{G}$, son

$\{y_3^3 - 1,\ y_2^2 + y_2y_3 + y_3^2,\ y_1 + y_2 + y_3,\ x_7 - y_3,\ x_4 - y_3,\ x_3 - y_3,\ x_9 - y_2,\ x_6 - y_2,$
$x_2 - y_2,\ x_8 + y_2 + y_3,\ x_5 + y_2 + y_3,\ x_1 + y_2 + y_3\}$.

En particular, los polinomios h_1 y h_2 son:

$$h_1(y_1, y_2, y_3) = y_1 + y_2 + y_3, \qquad h_2(y_2, y_3) = y_2^2 + y_2y_3 + y_3^2.$$

Ahora, si calculamos G, la base de Groebner reducida del ideal de 3-coloración del grafo $\mathcal{G}$, $I_{\mathcal{G},3}$, nos encontramos con que es precisamente la misma, teniendo en cuenta que las variables y_1, y_2 e y_3 se corresponden con x_{10}, x_{11} y x_{12} respectivamente.

$$\begin{aligned} G = \{&x_{12}^3 - 1, x_7 - x_{12}, x_4 - x_{12}, x_3 - x_{12}, x_{11}^2 + x_{11}x_{12} + x_{12}^2, x_9 - x_{11}, x_6 - x_{11} \\ &x_2 - x_{11}, x_{10} + x_{11} + x_{12}, x_8 + x_{11} + x_{12}, x_5 + x_{11} + x_{12}, x_1 + x_{11} + x_{12}\}. \end{aligned}$$

Esto nos indica que el grafo $\mathcal{G}$ admite una única 3-coloración, que salvo permutaciones de colores, es la dada al comienzo del ejemplo.

Ejemplo 3.18. Este procedimiento para determinar si un grafo es q-coloreable, o si posee una q-coloración única, también puede aplicarse a la resolución de Sudokus. Para esto, basta darse cuenta de que un Sudoku puede verse como un grafo.

El conjunto de vértices sería $V_S = \{1, \ldots, 81\}$, dado que cada cuadrado del Sudoku representa un vértice. Si dos cuadrados i, j pertenecen a la misma fila, a la misma columna o al mismo bloque de 3 x 3 cuadrados, entonces la arista (i, j) pertenecerá al conjunto de aristas, E_S. De esta forma, todos los vértices asociados a cuadrados que pertenecen a la misma fila, columna o bloque son adyacentes, y podemos considerar un Sudoku como un grafo $\mathcal{G}_S = (V_S, E_S)$.

Nuestro objetivo a la hora de resolver el Sudoku es dar una 9-coloración propia, con la única salvedad de que en este caso nuestros 'colores' serán los números del 1 al 9.

La forma de resolverlo es la siguiente:

- Consideramos el grafo $\mathcal{G}_S$ definido como acabamos de explicar.
- Asociamos a cada vértice i la variable x_i, con $i \in \{1, \ldots, 81\}$, y por cada dígito $j = 1, \ldots, 9$, buscamos un vértice i que tenga a j como dato inicial, y le cambiamos el nombre a x_i por y_j.
- Consideramos el ideal de 9-coloración del grafo, $I_{\mathcal{G},9}$.
- Le añadimos al ideal $I_{\mathcal{G},9}$ los 8 polinomios de la forma:

$$h_j(y_j, \ldots, y_9) = \sum_{\alpha_j + \ldots + \alpha_9 = j} y_j^{\alpha_j} \cdots y_9^{\alpha_9}, \text{ con } j \in \{1, \ldots, 8\}.$$

- Por cada dato adicional $j \neq 1$, que esté en un vértice i que no hemos renombrado por y_j, le añadimos al ideal $I_{\mathcal{G},9}$ el polinomio $x_i - y_j$.
- Por cada 1 adicional que tengamos como dato, que esté en un vértice i que no hemos renombrado por y_j, le añadimos al ideal $I_{\mathcal{G},9}$ el polinomio $x_i + y_2 + \ldots + y_9$.

Notemos que ahora el ideal $I_{\mathcal{G},9}$ consta de todos los polinomios $g_1, \ldots, g_n$ a los que se refiere el Teorema 3.16. Si el Sudoku está bien planteado, dicho teorema nos garantiza unicidad de 9-coloración y por tanto podremos resolverlo.

3.3. Criptosistemas Polly Cracker.

La criptografía se define como el conjunto de procedimientos y técnicas para escribir un mensaje de un modo enigmático, de forma que solo sea legible para quien sepa descifrarlo. A estos procedimientos se les denomina *criptosistemas*, y constan de dos etapas: la primera encripta el mensaje con una cierta clave, haciéndolo ilegible, y la segunda utiliza dicha clave para obtener el mensaje original.

Podemos clasificar los diferentes criptosistemas según sus claves:

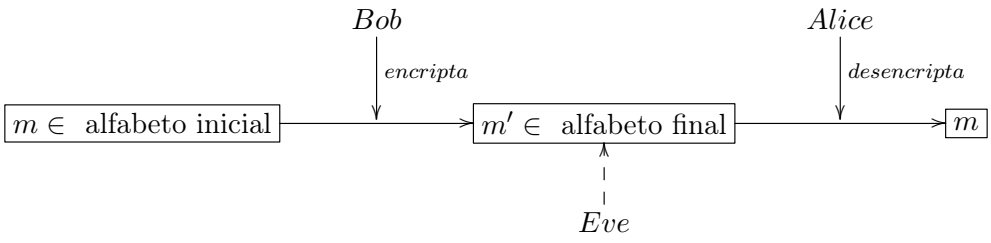
- Simétrico o de clave privada: Utiliza la misma clave para encriptar el mensaje y para desencriptarlo.
- Asimétrico o de clave pública: Usa dos claves diferentes. La clave de encriptado es pública, mientras que la de desencriptado no lo es.

Nos centraremos en el estudio de criptosistemas de clave pública, en particular en los *criptosistemas Polly Cracker*.

Desde el punto de vista matemático, el encriptado del mensaje consiste en una aplicación ε entre dos conjuntos a los que llamaremos *alfabeto inicial* y *alfabeto final*. Llamaremos mensaje a un elemento del alfabeto inicial, y su imagen a través de la aplicación ε será el mensaje encriptado. Por tanto, desencriptar un mensaje consiste en hallar la aplicación inversa de ε: ε^{-1}. La seguridad de un criptosistema depende de la dificultad de determinar la aplicación ε^{-1}.

Los criptosistemas Polly Cracker se caracterizan porque la clave pública que proporcionan es, o bien una base de Groebner de un polinomio en varias variables, o bien un punto de la variedad afín definida por un ideal.

Tenemos la siguiente situación: Bob quiere transmitirle un mensaje m a Alice sin que Eve pueda saber en qué consiste dicho mensaje. Para ello, Bob encripta m con la clave pública proporcionada por Alice, y transmite m'. Alice, conociendo la clave privada, debe ser capaz de recuperar m, pero Eve, que no posee más datos que los proporcionados por Bob, no.



El procedimiento que se ha de seguir para transmitir el mensaje, según el criptosistema *Polly Cracker abstracto*, es el siguiente: Alice toma un conjunto de polinomios F que generan un ideal I, del cuál conoce un cero, $\psi \in K^n$. Es decir, $\psi \in \mathbf{V}(I)$ o, equivalentemente, $f(\psi) = 0$ para todo $f \in I$. La clave que se hace pública en este caso es el conjunto de polinomios F que generan el ideal I, y la clave secreta es el punto ψ.

La forma de encriptar el mensaje $m \in K$ es la siguiente: Bob toma un polinomio arbitrario $h \in I$ y computa el mensaje encriptado, que es el polinomio $c := h + m$. Para obtener el mensaje original, Alice solo tiene que evaluar el polinomio en el punto ψ: $c(\psi) = h + m(\psi) = h(\psi) + m(\psi) = h(\psi) + m = m$.

La seguridad de este criptosistema se basa en la dificultad de hallar un cero del ideal I, es decir, en la dificultad de resolver un sistema de ecuaciones algebraicas. En la práctica, para asegurar que dicho sistema de ecuaciones no tenga una solución fácil de calcular en tiempo polinomial, se selecciona el conjunto de polinomios F de forma que sean una transcripción de un problema NP-completo, de forma que resolver el sistema de ecuaciones es equivalente a resolver este problema.

Los primeros en proponer estos criptosistemas fueron Koblitz y Fellows en 1994 [10]. Se basaron en problemas relacionados con la teoría de grafos, de hecho su idea inicial fue codificar el problema de 3-coloración de un grafo.

Ejemplo 3.19. Sea $\mathcal{G} = (V_\mathcal{G}, E_\mathcal{G})$ un grafo. Alice conoce una 3-coloración de este grafo, que, recordemos, es una aplicación $c : V_\mathcal{G} \longrightarrow \{1, 2, 3\}$ que verifica que si $(i, j) \in E_\mathcal{G}$ entonces $c(i) \neq c(j)$.

Para transmitir esta aplicación en lenguaje polinomial, se definen los conjuntos de polinomios F_0, F_1, F_2, F_3 en las variables $x_{i,k}$, dadas por $x_{i,k} = 1$ si $c(i) = k$, y $x_{i,k} = 0$ en caso contrario.

- $F_0 = \{x_{i,1} \cdot x_{i,2}, x_{i,1} \cdot x_{i,3}, x_{i,2} \cdot x_{i,3}, 1 \leqslant i \leqslant n\}$. Cada vértice no puede estar pintado de dos colores distintos.
- $F_1 = \{x_{i,1} + x_{i,2} + x_{i,3} - 1, 1 \leqslant i \leqslant n\}$. Cada vértice está pintado de al menos un color.
- $F_2 = \{x_{i,1} \cdot x_{j,1}, x_{i,2} \cdot x_{j,2}, x_{i,3} \cdot x_{j,3}, (i, j) \in E_\mathcal{G}\}$. Dos vértices conectados por una arista están pintados con colores distintos.
- $F_3 = \{x_{i,k}^2 - x_{i,k}, 1 \leqslant i \leqslant n, 1 \leqslant k, \leqslant 3\}$. Las variables $x_{i,k}$ sólo pueden tomar los valores 0 y 1, es decir, $x_{i,k} \in \mathbb{Z}_2$.

La clave pública es $F = F_0 \cup F_1 \cup F_2 \cup F_3$. Como ya vimos en la sección anterior, conocer una 3-coloración equivale a conocer un punto de la variedad afín definida por el ideal generado por F.

Observación 3.20. Es importante darse cuenta de que en la Sección: 3,2. Teoría de grafos, al hablar de la coloración de un grafo considerábamos únicamente una variable por cada vértice, mientras que en este caso estamos consideramos 3 variables por cada nodo. Esto provoca que necesitemos considerar más polinomios para generar el ideal de 3-coloración. Aunque esto podría parecer un inconveniente, en realidad para que la seguridad de nuestro criptosistema sea mayor nos conviene que sea difícil hallar los ceros del ideal.

Para presentar la clave pública se suele recurrir a la base de Groebner reducida del ideal generado por los polinomios de F.

En 1994, Barkee presentó un criptosistema Polly Cracker basado puramente en las bases de Groebner. La forma en la que él expresó este criptosistema se recoge en [11]. Al igual que en el caso del criptosistema Polly Cracker abstracto se trabaja en un cuerpo K, que usualmente será $\mathbb{F}_q$ de característica p, y en el anillo de polinomios en n variables con coeficientes en K, $K[x_1, \ldots, x_n]$.

Ahora, Bob desea enviarle un mensaje a Alice. Para esto, ella ha de crear su clave privada, y la clave pública. Para ello, considera un ideal I del anillo de polinomios $K[\boldsymbol{x}]$ del cual conoce una base de Groebner G. Dicha base será su clave privada. La clave pública será el ideal I y un subconjunto de formas normales $N = \{g_1, \ldots, g_r\}$ en $K[\boldsymbol{x}]$ respecto del ideal I.

Bob enviará un mensaje m, perteneciente en este caso a $K \cdot g_1 + \ldots + K \cdot g_r$. Para encriptarlo elegirá un polinomio $h \in I$ y calculará $c := h + m$. éste será el polinomio que le envíe a Alice.

Alice, para desencriptar el mensaje, debe hallar el resto del algoritmo de la división de c respecto a su base de Groebner. El funcionamiento de este criptosistema se fundamenta en que c es la suma de un elemento del ideal y el mensaje, compuesto por términos que provienen de formas normales respecto del ideal; esto implica que ningún monomio en m será divisible por el término principal de ningún polinomio de G. Entonces, Alice obtiene que el resto de la división es precisamente m.

Ejemplo 3.21. Bob quiere enviarle a Alice un mensaje. Para ello, Alice define el siguiente criptosistema en $\mathbb{Q}[x, y]$:

Alice toma el conjunto de polinomios $F = \{f_1 = x^3 - 2xy, f_2 = x^2y + x - 2y^2\}$, del cual conoce una base de Groebner del ideal I que genera F respecto al orden lexicográfico, con $x > y$:

$$G = \{f_1, f_2, f_3 = -x^2, f_4 = 2xy, f_5 = -x + 2y^2\}$$

La clave pública es el conjunto F y un subconjunto de formas normales en $\mathbb{Q}[x, y]$ respecto del ideal I. El soporte de las formas normales a de tener intersección vacía con el conjunto

$\{((3,0)+\mathbb{N}^2),((2,1)+\mathbb{N}^2),((2,0)+\mathbb{N}^2),((1,1)+\mathbb{N}^2),((1,0)+\mathbb{N}^2)\}$. Es decir, los exponentes de las formas normales no pueden ser estrictamente mayores que los exponentes del término principal de ningún polinomio de G con respecto al orden monomial que hemos seleccionado. Alice toma $N=\{y^2,y\}$.

Bob encripta el mensaje $m=3y^2+4y$ tomando el polinomio

$$h=f_1+f_2-2yf_4=x^3+x^2y-4xy^2-2xy+x-2y^2$$

y envía a Alice el polinomio $c=h+m=x^3+x^2y-4xy^2-2xy+x-2y^2+3y^2+4y$. Alice, para recuperar m, efectúa el algoritmo de la división y obtiene que:

$$c=h_1f_1+\ldots+h_5f_5+r=f_1+f_2+0\cdot f_3-2yf_4+0\cdot f_5+\overbrace{3y^2+4y}^{m}.$$

Los dos criptosistemas que acabamos de ver fueron los primeros Polly Cracker en ponerse en práctica. Posteriormente se estudiaron nuevos criptosistemas basados en las mismas ideas. Destaca entre ellos uno en el que resulta mucho más simple de encriptar un mensaje, en el sentido de que todas las elecciones son arbitrarias: el criptosistema *Polly Cracker concreto*.

En este método, Alice toma como clave privada un punto aleatorio $\psi\in K^n$. Para crear la clave pública, selecciona una serie de polinomios arbitrarios $f_1,\ldots,f_s$ y a partir de ellos crea los siguientes polinomios:

$$g_i=f_i-f_i(\psi).$$

El conjunto $\{g_1,\ldots,g_s\}$ será la clave pública de Alice. Bob, para encriptar un mensaje $m\in K$, toma s polinomios $h_1,\ldots,h_s$ del anillo de polinomios $K[x_1,\ldots,x_n]$ y a partir de ellos calcula $m'=\sum_{i=1}^{s}h_i\cdot g_i+m$. Este será el mensaje encriptado.

Alice, para desencriptar el mensaje, evalúa m' en el punto ψ, y esto le devuelve el mensaje original:

$$m'(\psi)=\sum_{i=1}^{s}h_i(\psi)\cdot g_i(\psi)+m(\psi)=\sum_{i=1}^{s}h_i(\psi)\cdot(f_i(\psi)-f_i(\psi))+m=m.$$

Bibliografía

[1] M. F. Atiyah, I. G. Macdonald. *Introducción al Álgebra Conmutativa.* Reverté, 1978.

[2] W. Fulton. *Algebraic Curves. An Introduction to Algebraic Geometry.* 2008.

[3] Cox, D.Little and O'Shea, *Ideals, Varieties and Algorithms. An introduction to Computational Algebraic Geometry and Commutative Algebra*, 2nd ed. Springer-Verlag, New York, 1992.

[4] Cox, D.Little and O'Shea, *Using Algebraic Geometry*, 3rd ed. Springer-Verlag, New York, 2007.

[5] Schauenburg, P. *A Gröbner–based treatment of elimination theory for affine varieties.* Journal of Symbolic Computation 42, 2007, 859-870.

[6] Buchberger B. *An algorithm for Finding a Basis for the Residue Class Ring of a Zero-Dimensional ideal.* Ph. D. Thesis, University of Innsbruck, Math. Inst., 1965.

[7] Windfeldt, T. *Computational Aspects of Graph Coloring and the Quillen–Suslin Theorem.* Ph. D. Thesis, University of Copenhagen, 2009.

[8] Hosten, R. Thomas. *Grobner bases and integer programming. Grobner Bases and Applications.* Ed. Buchberger and Winkler, Cambridge University Press, 1998. 144-157.

[9] Thomas, John B. *Applications of Computational Algebraic Geometry.* Ed. Cox and Sturmfels, AMS, Rhode Island, 1997. 119-140.

[10] Fellows, M. and Koblitz, N. *Combinatorial cryptosystems galore! Finite fields: theory, applications, and algorithms* (Las Vegas, NV, 1993), 51-61, Contemp. Math., 168, Amer. Math. Soc., Providence, RI, 1994.

[11] Barkee, B. et al. *Why you cannot even hope to use Gröbner bases in public key cryptography: an open letter to a scientist who failed and a challenge to those who have not yet failed.* Journal of Symbolic Computation 18 (1994), no. 6, 497-501.